SENATE SÉNAT

CANADA

First Session
Forty-second Parliament, 2015-16-17-18

*Proceedings of the Standing Senate Committee on*

# BANKING, TRADE AND COMMERCE

*Chair:*
The Honourable DOUGLAS BLACK

Wednesday, March 21, 2018
Thursday, March 22, 2018

Issue No. 36

*Seventh and eighth meetings:*

Study and report on issues and concerns pertaining to cyber security and cyber fraud

WITNESSES:
(*See back cover*)

Première session de la
quarante-deuxième législature, 2015-2016-2017-2018

*Délibérations du Comité sénatorial permanent des*

# BANQUES ET DU COMMERCE

*Président :*
L'honorable DOUGLAS BLACK

Le mercredi 21 mars 2018
Le jeudi 22 mars 2018

Fascicule nº 36

*Septième et huitième réunions :*

Étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude

TÉMOINS :
(*Voir à l'endos*)

53884-53896

STANDING SENATE COMMITTEE ON BANKING, TRADE AND COMMERCE

The Honourable Douglas Black, *Chair*

The Honourable Carolyn Stewart Olsen, *Deputy Chair*

and

The Honourable Senators:

Dagenais
* Day
(or Mercer)
* Harder, P.C.
(or Bellemare)
(or Mitchell)
Marshall
Marwah
Ringuette
* Smith
(or Martin)
Tkachuk
Unger
Wallin
Wetston
* Woo
(or Saint-Germain)

*Ex officio members

(Quorum 4)

*Changes in membership of the committee:*

Pursuant to rule 12-5 and to the order of the Senate of November 7, 2017, membership of the committee was amended as follows:

The Honourable Senator Marshall replaced the Honourable Senator MacDonald (*March 22, 2018*).

The Honourable Senator MacDonald replaced the Honourable Senator Tannas (*March 20, 2018*).

COMITÉ SÉNATORIAL PERMANENT DES BANQUES ET DU COMMERCE

*Président :* L'honorable Douglas Black

*Vice-présidente :* L'honorable Carolyn Stewart Olsen

et

Les honorables sénateurs :

Dagenais
* Day
(ou Mercer)
* Harder, C.P.
(ou Bellemare)
(ou Mitchell)
Marshall
Marwah
Ringuette
* Smith
(ou Martin)
Tkachuk
Unger
Wallin
Wetston
* Woo
(ou Saint-Germain)

* Membres d'office

(Quorum 4)

*Modifications de la composition du comité :*

Conformément à l'article 12-5 du Règlement et à l'ordre adopté par le Sénat le 7 novembre 2017, la liste des membres du comité est modifiée, ainsi qu'il suit :

L'honorable sénatrice Marshall a remplacé l'honorable sénateur MacDonald (*le 22 mars 2018*).

L'honorable sénateur MacDonald a remplacé l'honorable sénateur Tannas (*le 20 mars 2018*).

Published by the Senate of Canada
Available on the Internet: http://www.parl.gc.ca

Publié par le Sénat du Canada
Disponible sur internet : http://www.parl.gc.ca

## MINUTES OF PROCEEDINGS

OTTAWA, Wednesday, March 21, 2018
(91)

[*English*]

The Standing Senate Committee on Banking, Trade and Commerce met this day at 4:18 p.m., in room 9, Victoria Building, the chair, the Honourable Douglas Black, presiding.

*Members of the committee present:* The Honourable Senators Black (*Alberta*), Dagenais, MacDonald, Marwah, Ringuette, Stewart Olsen, Tkachuk, Unger, Wallin and Wetston (10).

*In attendance:* Brett Stuckey and Adriane Yong, Analysts, Parliamentary Information and Research Services, Library of Parliament; Mila Pavlovic, Communications Officer, Senate Communications Directorate.

*Also present:* The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, October 17, 2017, the committee continued its study on issues and concerns pertaining to cyber security and cyber fraud. *(For complete text of the order of reference, see proceedings of the committee, Issue No. 26.)*

*WITNESSES:*

*Cybersecurity and Privacy Institute, University of Waterloo:*

Florian Kerschbaum, Interim Director.

*Public Safety Canada:*

Colleen Merchant, Director General, National Cyber Security Directorate.

*Royal Canadian Mounted Police:*

Chief Superintendent Jeff Adam, Acting Assistant Commissioner, Technical Operations.

*Communications Security Establishment:*

André Boucher, Associate Deputy Chief, IT Security.

The chair made a statement.

Mr. Kerschbaum made a statement and answered questions.

At 5:12 p.m., the committee suspended.

At 5:17 p.m., the committee resumed.

Ms. Merchant, Chief Superintendent Adam and Mr. Boucher each made a statement and answered questions.

At 6:20 p.m., the committee adjourned to the call of the chair.

*ATTEST:*

## PROCÈS-VERBAUX

OTTAWA, le mercredi 21 mars 2018
(91)

[*Français*]

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 16 h 18, dans la pièce 9 de l'édifice Victoria, sous la présidence de l'honorable Douglas Black (*président*).

*Membres du comité présents :* Les honorables sénateurs Black (*Alberta*), Dagenais, MacDonald, Marwah, Ringuette, Stewart Olsen, Tkachuk, Unger, Wallin et Wetston (10).

*Également présents :* Brett Stuckey et Adriane Yong, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement; Mila Pavlovic, agente de communications, Direction des communications.

*Aussi présents :* Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 17 octobre 2017, le comité poursuit son étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude. *(Le texte intégral de l'ordre de renvoi figure au fascicule nº 26 des délibérations du comité.)*

*TÉMOINS :*

*Institut de la cybersécurité et de la protection des renseignements personnels, Université de Waterloo :*

Florian Kerschbaum, directeur intérimaire.

*Sécurité publique Canada :*

Colleen Merchant, directrice générale, Direction de la cybersécurité nationale.

*Gendarmerie royale du Canada :*

Surintendant principal Jeff Adam, commissaire adjoint par intérim, Opérations techniques.

*Centre de la sécurité des télécommunications :*

André Boucher, chef adjoint associé, Sécurité des TI.

Le président fait une déclaration.

M. Kerschbaum fait une déclaration et répond aux questions.

À 17 h 12, la séance est suspendue.

À 17 h 17, la séance reprend.

Mme. Merchant, le surintendant principal Adam et M. Boucher font chacun une déclaration et répondent aux questions.

À 18 h 20, la séance est levée jusqu'à nouvelle convocation de la présidence.

*ATTESTÉ :*

OTTAWA, Thursday, March 22, 2018
(92)

[*English*]

The Standing Senate Committee on Banking, Trade and Commerce met this day at 11:30 a.m., in room 9, Victoria Building, the chair, the Honourable Douglas Black, presiding.

*Members of the committee present:* The Honourable Senators Black (*Alberta*), Dagenais, Marshall, Marwah, Ringuette, Stewart Olsen, Tkachuk, Unger, Wallin and Wetston (10).

*In attendance:* Adriane Yong and Brett Stuckey, Analysts, Parliamentary Information and Research Services, Library of Parliament; Mila Pavlovic, Communications Officer, Senate Communications Directorate.

*Also present:* The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, October 17, 2017, the committee continued its study on issues and concerns pertaining to cyber security and cyber fraud. *(For complete text of the order of reference, see proceedings of the committee, Issue No. 26.)*

*WITNESS:*

*Morrison & Foerster LLP:*

John P. Carlin, Chair, Global Risk and Crisis Management (by video conference).

The chair made a statement.

Mr. Carlin made a statement and answered questions.

At 12:37 p.m., the committee adjourned to the call of the chair.

*ATTEST:*

OTTAWA, le jeudi 22 mars 2018
(92)

[*Français*]

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 11 h 30, dans la pièce 9 de l'édifice Victoria, sous la présidence de l'honorable Douglas Black (*président*).

*Membres du comité présents :* Les honorables sénateurs Black (*Alberta*), Dagenais, Marshall, Marwah, Ringuette, Stewart Olsen, Tkachuk, Unger, Wallin et Wetston (10).

*Également présents :* Adriane Yong et Brett Stuckey, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement; Mila Pavlovic, agente de communications, Direction des communications.

*Aussi présents :* Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 17 octobre 2017, le comité poursuit son étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude. *(Le texte intégral de l'ordre de renvoi figure au fascicule nº 26 des délibérations du comité.)*

*TÉMOIN :*

*Morrison & Foerster s.r.l. :*

John P. Carlin, président, Risques mondiaux et gestion de crise (par vidéoconférence).

Le président fait une déclaration.

M. Carlin fait une déclaration et répond aux questions.

À 12 h 37, la séance est levée jusqu'à nouvelle convocation de la présidence.

*ATTESTÉ :*

*La greffière du comité,*

Barbara Reynolds

*Clerk of the Committee*

## EVIDENCE

OTTAWA, Wednesday, March 21, 2018

The Standing Senate Committee on Banking, Trade and Commerce met this day at 4:18 p.m. to study and report on issues and concerns pertaining to cyber security and cyber fraud.

**Senator Douglas Black** (*Chair*) in the chair.

[*English*]

**The Chair:** Good afternoon and welcome, colleagues, and members of the general public, who are following today's proceedings of the Standing Senate Committee on Banking, Trade and Commerce here in the room or listening via the Web. My name is Doug Black. I'm a senator from Alberta, and I have the privilege of chairing this committee.

I would like to call upon my colleagues to introduce themselves, starting, please, with Senator Unger.

**Senator Unger:** I'm Betty Unger from Edmonton, Alberta .

**Senator Wallin:** Pamela Wallin, senator from Saskatchewan.

**Senator Ringuette:** Pierette Ringuette from New Brunswick.

**Senator Marwah:** Sabi Marwah, Ontario.

**Senator Wetston:** Howard Wetston, Ontario.

**Senator Stewart Olsen:** Carolyn Stewart Olsen, New Brunswick.

**Senator MacDonald:** Michael MacDonald from Nova Scotia.

**The Chair:** We're also, as we always are, very ably assisted by our clerk and our analysts from the Library of Parliament.

Today, we are continuing our study on issues and concerns pertaining to cybersecurity and cyber fraud, including cyberthreats to Canada's financial and commercial sectors, the current state of cybersecurity technologies and cybersecurity measures and regulations in Canada and abroad. I'm pleased to welcome Dr. Florian Kerschbaum, who is the Interim Director of the Cybersecurity and Privacy Institute at the University of Waterloo and an associate professor in the School of Computer Science at that university.

## TÉMOIGNAGES

OTTAWA, le mercredi 21 mars 2018

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 16 h 18, afin d'étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude.

**Le sénateur Douglas Black** (*président*) occupe le fauteuil.

[*Traduction*]

**Le président :** Bonjour et bienvenue à mes collègues ainsi qu'aux membres du grand public qui sont présents dans la salle ou qui suivent les délibérations du Comité sénatorial permanent des banques et du commerce sur le Web. Je m'appelle Doug Black. Je suis un sénateur de l'Alberta et j'ai le privilège de présider ce comité.

Je demanderais maintenant à mes collègues de se présenter à tour de rôle, en commençant par la sénatrice Unger.

**La sénatrice Unger :** Je m'appelle Betty Unger et je suis d'Edmonton, en Alberta.

**La sénatrice Wallin :** Pamela Wallin, sénatrice de la Saskatchewan.

**La sénatrice Ringuette :** Pierrette Ringuette du New Brunswick.

**Le sénateur Marwah :** Sabi Marwah, Ontario.

**Le sénateur Wetston :** Howard Wetston, Ontario.

**La sénatrice Stewart Olsen :** Carolyn Stewart Olsen, Nouveau-Brunswick.

**Le sénateur MacDonald :** Michael MacDonald de la Nouvelle-Écosse.

**Le président :** Comme toujours, nous pouvons également compter sur les excellents services de notre greffière et de nos analystes de la Bibliothèque du Parlement.

Nous poursuivons aujourd'hui notre étude des questions et des préoccupations relatives à la cybersécurité et à la cyberfraude, y compris les menaces cybernétiques qui pèsent sur les secteurs financier et commercial du Canada, la situation actuelle relative aux technologies de cybersécurité, et les mesures et règlements en matière de cybersécurité au Canada et à l'étranger. J'ai le plaisir de souhaiter la bienvenue à M. Florian Kerschbaum, directeur par intérim de l'Institut de la cybersécurité et de la protection des renseignements personnels de l'Université de Waterloo, qui est également professeur agrégé à la faculté de l'informatique de la même université.

I want to also report to senators that you may recall that Mr. Kerschbaum was scheduled to appear last October, but the meeting was cancelled. So, Doctor, if you can start with your opening statement, after your presentation, we will look forward to questions and answers with you.

Thank you very much for being here.

**Florian Kerschbaum, Interim Director, Cybersecurity and Privacy Institute, University of Waterloo:** Thank you.

Dear members of the Senate, it is my pleasure to speak to the Standing Senate Committee on Banking, Trade and Commerce on cybersecurity today. I am Associate Professor of Computer Science at the University of Waterloo and director of the university's institute on cybersecurity and privacy, the Waterloo CPI. I joined the University of Waterloo recently, in January 2017, and before I was working for 11 years at the European software vendor SAP, in Germany.

I want to speak to three issues on the current state of cybersecurity technologies today.

First, the fundamental difficulty of cyberdefence. This means why is it so much harder to defend than attack?

Second, the unfavourable incentives for cybersecurity in industry and government. This means why do companies not invest enough to stop the problem, and how the government may help.

Third, the need for fundamental research and education on cybersecurity challenges. This means why is science a component of the cybersecurity puzzle and how it may help to change the landscape.

Let me start with cyberdefence. It is crucial to understand that cyberdefence is much harder than cyberattack. Whereas the attacker has to find only one vulnerability, the defender has to close all possible attack paths. This imbalance makes the task for the defender much more difficult and necessitates disproportionate investments in cyberdefence compared to the budget available for the attacker.

Our only strategy to deal with the inherent insecurity of computer systems is the defence in-depth. This means that, as it should be protected by multiple layers of security mechanisms, once the attacker has broken one control, there should be another in place to uphold the defence. This is rarely deployed in

Je veux rappeler à mes collègues sénateurs que M. Kerschbaum devait comparaître devant nous en octobre dernier, mais que la séance en question a dû être annulée. Monsieur Kerschbaum, je vais donc vous laisser la parole pour vos observations préliminaires, après quoi nous passerons aux questions des membres du comité.

Merci beaucoup d'être des nôtres aujourd'hui.

**Florian Kerschbaum, directeur par intérim, Institut de la cybersécurité et de la protection des renseignements personnels, Université de Waterloo :** Merci.

Mesdames et messieurs les sénateurs, je suis heureux de témoigner aujourd'hui devant le Comité sénatorial permanent des banques et du commerce pour vous parler de cybersécurité. Je suis professeur agrégé en informatique à l'Université de Waterloo et directeur de l'Institut de la cybersécurité et de la protection des renseignements personnels de cette université. Je suis à l'emploi de celle-ci depuis janvier 2017 seulement. Auparavant, j'ai travaillé pendant 11 ans en Allemagne pour la société SAP, un distributeur de logiciels européen.

Je vais me pencher aujourd'hui sur trois aspects de la situation actuelle des technologies de cybersécurité.

Il y a premièrement la principale difficulté liée à la cyberdéfense, à savoir le fait qu'il est beaucoup plus difficile de se défendre que d'attaquer.

Deuxièmement, il y a un manque d'incitatifs pour la cybersécurité dans l'industrie et au sein du gouvernement. Autrement dit, il faut se demander pourquoi les entreprises n'investissent pas suffisamment pour enrayer le problème et ce que le gouvernement pourrait faire pour changer les choses.

Troisièmement, il faut noter l'importance de la recherche fondamentale sur les défis liés à la cybersécurité ainsi que de l'éducation dans ce domaine. Il s'agit de savoir en quoi la science est une pièce du casse-tête de la cybersécurité et comment elle peut contribuer à améliorer la situation.

Je vais d'abord parler de cyberdéfense. Il est essentiel de comprendre qu'il est beaucoup plus difficile d'assurer la cyberdéfense d'un système que de mener des cyberattaques. Alors qu'il suffit aux pirates informatiques de trouver une seule faille, les victimes de leurs attaques doivent bloquer tous les points d'accès possibles. Ce déséquilibre rend la tâche des responsables de la sécurité des systèmes beaucoup plus ardue et les oblige à consacrer à la cyberdéfense des sommes démesurées par rapport aux fonds nécessaires aux pirates.

Notre seule stratégie pour contrer la vulnérabilité inhérente des systèmes informatiques est la défense en profondeur qui consiste à mettre en place de multiples couches de mécanismes de sécurité et à déployer un nouveau mécanisme toutes les fois qu'un pirate réussit à en contourner un. Or, comme je

practice, and I will speak to this next. It is also not fundamentally understood at the scientific level, and I will speak to this later.

If we accept cybersecurity requires significant effort, we can ask: Why are we discussing this at a policy level in this specific committee?

While it is clear from a national level that we want to defend our vital and critical infrastructures from disruptions and theft by attackers in criminal organizations or agents and nation-state actors, markets do not reward good cybersecurity. Cybersecurity is the absence of bad events and not the presence of positive features.

Only niche players compete on security and privacy in their products. Major data breaches have no long-term effect on stock prices or consumer behaviour. In fact, companies have turned their bad cybersecurity into market opportunities, such as identity theft insurance.

As a consequence, companies are not innovating on cybersecurity but only make minimum investments to keep the business going and maintain a perception of privacy. As with the attacking bear, one does not have to outrun the bear but only the competitor. Again, from an outside perspective, it is clear the attacker will catch someone, and from time to time that someone will be in Canada, particularly considering how many bears there are in Canada. My apologies for the joke.

The lack of industrial innovation in cybersecurity is critical. Even when turning to the venture capital market, one is often confronted with the statement "Customers do not pay for security."

An alternative would be regulation. However, the government's role in this is unclear. Law enforcement and intelligence agencies are allowing for trivial access to personal data. It is important to understand that this lack of privacy correlates with weak cybersecurity and contradicts defence in-depth. When a government body can access the data, so can a skilled attacker. While this essentially zero-cost access to data clearly facilitates cheaper law enforcement and intelligence, these agencies have been solving crimes and collecting data before there were smartphones and the Internet. Even with strong encryption, it is still possible to intercept the data at the source.

l'expliquerai dans quelques instants, la défense en profondeur est rarement mise en œuvre dans la pratique. De plus, elle n'est pas très bien comprise au niveau scientifique; j'aborderai aussi cette question un peu plus tard.

Si on reconnaît que la cybersécurité exige des efforts considérables, on peut alors se demander pourquoi nous abordons la question d'un point de vue stratégique devant votre comité.

Même si, à l'échelle nationale personne ne remet en question la pertinence de protéger nos infrastructures essentielles contre les attaques et le vol de données perpétrés par des pirates faisant partie d'organisations criminelles ou des agents d'États-nations, les marchés ne récompensent pas les bonnes pratiques en matière de cybersécurité. Pour plusieurs, la cybersécurité, c'est l'absence d'activités néfastes, et non pas la présence de caractéristiques positives.

Seules les entreprises spécialisées incluent de véritables options de sécurité et de protection des renseignements dans leurs produits. Les graves atteintes à la protection des données n'ont pas d'effet à long terme sur le cours des actions ou le comportement des consommateurs. En fait, des entreprises ont profité de leurs mauvaises pratiques en matière de cybersécurité pour créer de nouveaux débouchés tels que l'assurance contre le vol d'identité.

C'est pourquoi les entreprises ne cherchent pas à innover dans le domaine de la cybersécurité. Elles se contentent d'investir le minimum pour assurer la poursuite des activités et donner une impression de protection des renseignements. Un peu comme quand un ours passe à l'attaque, l'important, ce n'est pas de courir plus vite que l'ours, mais bien de courir plus vite que les autres proies. Dans le fond, les cyberattaquants finissent toujours par trouver une proie et, à l'occasion, cette proie se trouve au Canada — ce qui n'est pas surprenant, compte tenu de tous les ours qui vivent dans ce pays — pardonnez-moi mon humour.

Le manque d'innovation en cybersécurité de la part de l'industrie est grave. Même dans le marché du capital-risque, on entend souvent dire que « les clients ne paient pas pour la sécurité ».

La réglementation pourrait représenter une solution, mais le rôle du gouvernement à cet égard n'est pas clair. Les organismes d'application de la loi et du renseignement réclament un accès plus facile aux données personnelles. Il est important de comprendre qu'en affaiblissant la protection des renseignements personnels, on affaiblit également la cybersécurité et on mine l'efficacité de la défense en profondeur. Lorsqu'on permet à un organisme gouvernemental d'avoir accès aux données, on ouvre du même coup la porte aux cyberattaquants habiles. Il est clair que l'accès pratiquement gratuit aux données permet aux organismes d'application de la loi et du renseignement de travailler à moindre coût, mais ces organismes arrivaient à résoudre des crimes et à collecter des renseignements avant

même l'avènement des téléphones intelligents et d'Internet. Il est possible d'intercepter des données à la source, même lorsque de solides mesures de chiffrement sont en place.

If we accept that the situation of cybersecurity innovation is bleak, we can ask what we can do about it. As a researcher, I see fundamental challenges in overcoming the current situation.

Si l'on reconnaît que la situation de l'innovation en cybersécurité est peu reluisante, on peut se demander ce qu'on peut faire pour corriger la situation actuelle. En tant que chercheur, j'estime qu'il faudra pour ce faire relever des défis fondamentaux.

First, much of cybersecurity in practice uses a "break, fix and break again" methodology. Security researchers have discovered attacks which are, in turn, fixed by modifying or patching the system to prevent the specific attack, yet the system is broken again in a short time, often by only a very slightly modified attack.

D'abord, la majorité des pratiques et de la recherche liées à la cybersécurité sont fondées sur le cycle violation, correction, nouvelle violation. Lorsque les spécialistes de la sécurité détectent des attaques, ils modifient ou réparent le système pour corriger les failles et empêcher une autre attaque du même genre. Malgré cela, le système est de nouveau corrompu peu de temps après, souvent à cause d'une attaque à peine différente de la première.

I see the need for fundamental research that addresses these challenges at the root cause and not only operates at the surface with minimal investment. These challenges to cybersecurity are fundamental scientific challenges that require basic research on the science of cybersecurity. For example, how do we develop secure software in the presence of human programmers? What does it mean to be secure?

À mon avis, plutôt que de simplement nous attaquer au problème de façon superficielle en y consacrant le moins de fonds possible, nous devons miser sur la recherche fondamentale afin de régler le problème à la source. Pour relever les défis liés à la cybersécurité, il faut recourir à la recherche scientifique fondamentale sur la science de la cybersécurité et chercher à comprendre, par exemple, comment concevoir un logiciel sécurisé en présence de programmeurs humains ou ce que l'on entend par « sécurisé ».

If we look beyond Canada's borders, the United States have established NSA Centers of Academic Excellence and funded many IARPA, Intelligence Advanced Research Projects Activity, programs that enhance fundamental cybersecurity technologies from theoretical concepts to practical useability.

Si l'on regarde ce qui se fait à l'étranger, on voit que les États-Unis ont créé les centres d'excellence universitaires de la National Security Agency et qu'ils financent de nombreux programmes de l'IARPA (Intelligence Advanced Research Projects Activity) qui visent à améliorer les technologies fondamentales de cybersécurité, depuis les concepts théoriques jusqu'à des produits concrets.

My home country, Germany, has established a Helmholtz national institute, and plans are under way for a Max Planck Institute on the science of cybersecurity.

L'Allemagne, mon pays d'origine, a mis sur pied un institut national Helmholtz et prévoit ouvrir un institut Max-Planck consacré à la science de la cybersécurité.

I argue that without a change in incentives, industry will not step up to these challenges. The University of Waterloo has an internationally recognized profile in cybersecurity. Its newly established Cybersecurity and Privacy Institute, the Waterloo CPI, is well positioned to tackle these challenges using the required interdisciplinary approaches. We have established a first relationship with the Royal Bank of Canada and have about 40 faculty members working on cybersecurity and privacy challenges.

Comme je l'ai souligné, si on n'améliore pas les incitatifs offerts, l'industrie ne cherchera pas à relever ces défis. L'Université de Waterloo est reconnue mondialement dans le domaine de la cybersécurité. Son nouvel Institut de la cybersécurité et de la protection des renseignements personnels est bien placé pour s'attaquer à ces défis en adoptant l'approche interdisciplinaire voulue. Nous avons établi un premier partenariat avec la Banque Royale du Canada, et une quarantaine de membres de notre corps professoral se penchent sur les problèmes de cybersécurité ou de protection des renseignements personnels.

Canada's research funding is excellent at combining industry interests with scientific objectives, but we may need to do more here. In order for Canada to stay competitive in the science of cybersecurity, seed government funding may be needed, be it in

Au Canada, le financement de la recherche permet de conjuguer intérêts de l'industrie et objectifs scientifiques, mais nous pourrions devoir en faire davantage. Pour que le Canada puisse demeurer concurrentiel dans le domaine de la science de

the form of Centres of Excellence or Lighthouse Projects. A national Centre of Excellence could promote Canada's reputation in cybersecurity research and help educate the necessary personnel for enhanced investment in cybersecurity. The results from basic research can then be used to change the landscape of cybersecurity in Canada's banking, trade and commerce, for example, by leveraging the next generation of cybersecurity leaders, and overcoming the fundamental challenges we currently face.

la cybersécurité, il pourrait être nécessaire que le gouvernement accorde du financement de démarrage, que ce soit pour des centres d'excellence ou des projets phares. Un centre national d'excellence pourrait mousser la réputation du Canada en matière de recherche en cybersécurité et contribuer à sensibiliser les personnes voulues à l'importance d'accroître les fonds investis en la matière. Les fruits de la recherche fondamentale pourraient ensuite servir à modifier le portrait de la cybersécurité dans les domaines des banques et du commerce au Canada, notamment en favorisant l'essor de la prochaine génération de chefs de file en cybersécurité et en nous permettant de surmonter les défis fondamentaux devant lesquels nous nous trouvons actuellement.

The University of Waterloo has many computer-oriented majors at the bachelor's and master's level that have cybersecurity as an elective component, but no dedicated computer security major. This may change over time with increased investment by industry and the government. However, we already educate several PhDs in computer security and privacy each year. I am confident the University of Waterloo Cybersecurity and Privacy Institute can play a crucial role in fostering Canada's cybersecurity education, science and innovation.

L'Université de Waterloo offre de nombreux programmes en informatique au niveau du baccalauréat et de la maîtrise qui comprennent des cours optionnels axés sur la cybersécurité, mais elle n'a encore aucun programme avec spécialisation en sécurité informatique. Cela pourrait changer si l'industrie et le gouvernement accroissent leur financement. Nous formons cependant plusieurs doctorants en sécurité informatique et en protection des renseignements chaque année. Je suis convaincu que l'Institut de la cybersécurité et de la protection des renseignements personnels de l'Université de Waterloo peut jouer un rôle crucial dans l'éducation, la science et l'innovation liées à la cybersécurité au Canada.

**The Chair:** Thank you very much. We will move to questions. Senator Stewart Olsen, please.

**Le président :** Merci beaucoup. Nous passons aux questions, en commençant par la sénatrice Stewart Olsen.

**Senator Stewart Olsen:** Thank you for being here. I'm very pleased to hear what you've had to say. That has been one of the main things I'm questioning on. It really does have to do with the need to train good cybersecurity people, and beginning at a lower level than university. I'm pleased that Waterloo is doing some training, but I do believe there should be a major, and I think we have to push for it.

**La sénatrice Stewart Olsen :** Merci beaucoup de votre présence aujourd'hui. Je suis ravie de ce que j'ai pu entendre jusqu'à maintenant. Cela fait partie des sujets qui m'intéressent au plus haut point. Il est vraiment important de pouvoir former d'excellents spécialistes en cybersécurité en se mettant à la tâche avant même l'université. Je me réjouis de voir l'Université de Waterloo offrir de la formation, mais je crois vraiment qu'il devrait y avoir un programme avec spécialisation, et j'estime que nous devrions exercer des pressions en ce sens.

What are your thoughts on how to encourage this to move forward? Is it a lack of identifying cybersecurity analyst as a job for young people? Bringing it right down to the basics, why did you get into it, or why would young people want to do this? Because we need this, obviously.

Selon vous, comment devrions-nous nous y prendre pour réaliser des progrès à ce chapitre? Faudrait-il sensibiliser davantage les jeunes à la possibilité de faire carrière comme analyste en cybersécurité? Il faudrait leur expliquer bien clairement les raisons pour lesquelles une telle carrière pourrait les intéresser, car nous avons manifestement besoin de nouvelles ressources.

**Mr. Kerschbaum:** Thank you. That's a very good question.

**M. Kerschbaum :** Merci pour cette excellente question.

There are a couple of components to this. First of all, there are certainly a number of jobs that relate to cybersecurity. These jobs usually pay very well, even compared to regular computer science jobs. There is definitely a demand in the labour market. I'm not sure whether or not we need to operate on that level.

Il y a quelques aspects à considérer. Précisons d'abord qu'il y a déjà un certain nombre d'emplois liés à la cybersécurité. Ces emplois sont habituellement très bien rémunérés, même en comparaison avec les autres secteurs de l'informatique. Il y a assurément une demande sur le marché du travail. Je ne sais donc pas s'il est vraiment nécessaire d'intervenir à ce niveau.

Then there is the question how can we educate people to do this? Cybersecurity is a very multifaceted interdisciplinary problem. One the challenges the University of Waterloo faces is combining the different skills from the professors on this aspect. The cybersecurity institute may help here. However, when I look at computer science, it may be necessary to strengthen certain aspects of security, for example software or network security, more than we currently have.

The third aspect is what would motivate someone to become a cybersecurity specialist? In my courses, I sometimes talk about the mind of a security specialist, which is very much this notion of trying to find flaws, thinking outside of the box and trying to break things. There are certainly people who are predestined to do this. We may want to foster this maybe even at an earlier stage, as you mentioned.

At the high school level, the first and most important thing is to raise awareness for cybersecurity. To make sure people are not bothered by having to unlock their phone or enter a password but understand this is a necessity in order to protect their data. We are very happy at the University of Waterloo to have that for the undergrad course, which is very popular with the students, but to turn this into a program, additional effort is needed.

**Senator Wetston:** Thank you for being here today.

I'd like to ask a couple of general questions. Your description of the cybersecurity brain and the people who have that remind me of saying I don't want to be an actuary either. I can't manage the granular questions in this area but I'll ask a couple of general ones.

Obviously, you worked in Germany for a number of years. Germany is a highly industrialized nation with a great deal of science and research. Can you tell me whether or not you believe Germany is much further ahead than Canada with respect to the cybersecurity? If so, what would be the basis for you being able to support that point of view?

**Mr. Kerschbaum:** Let me answer that in two aspects. In the aspect of cybersecurity as a country, I'm probably not the best witness for you. I know that Germany has what is called the BSI, the German computer security institute, which is in the department of state responsible for enhancing the cybersecurity in the government and also for supporting the public sector. However, I'm not the expert to compare that.

Il y a ensuite la question de la formation à proprement parler. La cybersécurité est une matière interdisciplinaire qui renferme de multiples facettes. Il est notamment difficile pour l'Université de Waterloo de combiner les compétences de ses différents professeurs à cette fin. L'Institut de la cybersécurité pourra éventuellement nous faciliter les choses. Il faudra peut-être toutefois s'employer à renforcer certaines compétences en sécurité informatique, par exemple par rapport aux logiciels et aux réseaux, comparativement à ce qui est disponible actuellement.

Il faut se demander en troisième lieu ce qui peut motiver quelqu'un à devenir spécialiste en cybersécurité. Il m'arrive de traiter dans mes cours de la tournure d'esprit d'un spécialiste en sécurité qui doit très souvent chercher à déceler des lacunes, à voir les choses sous un angle différent et à tout décortiquer. Il y a assurément des gens qui ont toutes les prédispositions voulues pour ce faire. Nous pourrions sans doute essayer de les mobiliser encore plus tôt, comme vous l'avez suggéré.

Au niveau de l'école secondaire, il faut d'abord et avant tout s'assurer de sensibiliser les jeunes à l'importance de la cybersécurité. Il faut voir à ce que chacun ne soit pas ennuyé par le fait de devoir déverrouiller son téléphone ou saisir un mot de passe, mais qu'il comprenne plutôt que c'est absolument nécessaire pour protéger ses données. Nous sommes très heureux d'offrir cette formation au niveau du baccalauréat à l'Université de Waterloo, car les étudiants l'apprécient beaucoup, mais il faudra un effort additionnel pour en faire un programme avec spécialisation.

**Le sénateur Wetston :** Je vous remercie de votre présence.

J'aimerais vous poser deux ou trois questions d'ordre général. Ce que vous dites sur les génies de la cybersécurité me rappelle que j'ai déjà dit ne pas vouloir être actuaire non plus. Je ne peux pas poser des questions complexes sur le sujet, mais je vais en poser deux ou trois d'ordre général.

Évidemment, vous avez travaillé en Allemagne pendant un certain nombre d'années. C'est une nation très industrialisée où beaucoup de travaux scientifiques sont faits. Pouvez-vous me dire si, selon vous, l'Allemagne est beaucoup plus avancée que le Canada sur le plan de la cybersécurité? Si c'est le cas, sur quoi repose votre point de vue?

**M. Kerschbaum :** Permettez-moi de vous répondre en deux volets. En ce qui concerne la cybersécurité au pays, je ne suis probablement pas le témoin idéal pour répondre à la question. Je sais qu'en Allemagne, il y a ce qu'on appelle le BSI, l'institut de sécurité informatique, qui fait partie du ministère responsable d'améliorer la cybersécurité au gouvernement et également d'appuyer le secteur public. Toutefois, je ne suis pas un spécialiste qui serait en mesure de faire cette comparaison.

Let me go to the second step which I can talk about, namely, research on cybersecurity. In that respect, I think Germany is way ahead. Germany has a couple of centres in cybersecurity that are internationally recognized in the universities at Bochum, Darmstadt and maybe also in Karlsruhe or Munich, whereas in Canada at the international level it is probably only the University of Waterloo. The institutes I mentioned on the fundamental aspects of security research, I think they make it easier for researchers to invest in.

Permettez-moi de passer à l'autre volet, dont je peux parler, c'est-à-dire la recherche sur la cybersécurité. À mon avis, l'Allemagne est bien en avance sur le Canada à ce chapitre. Elle compte deux ou trois centres sur la cybersécurité reconnus à l'échelle internationale, à Bochum, à Darmstadt et peut-être également à Karlsruhe ou à Munich, tandis qu'au Canada, il n'y a probablement que l'Université de Waterloo qui est reconnue à l'échelle internationale. Dans les instituts que j'ai mentionnés, je crois qu'il est plus facile pour les chercheurs d'investir dans les aspects fondamentaux de la recherche sur la sécurité.

**Senator Wetston:** Let me ask you a more practical question in the sense of attack and defend. We had some witnesses here previously and I recall asking a question about is it simply about defending as you would in a sport or is it about offence, or attacking. We did get a response. I don't know if you have had a chance to review the transcript, but maybe you might review what he said.

**Le sénateur Wetston :** Permettez-moi de vous poser une question plus concrète en ce sens qu'elle porte sur l'offensive et la défensive. Des témoins ont comparu précédemment et je me rappelle leur avoir demandé s'il s'agissait simplement d'une question de défensive, comme dans le sport, ou d'offensive. Ils nous ont répondu. J'ignore si vous avez eu l'occasion de lire la transcription de la réunion, mais vous pourriez peut-être regarder ce que la personne a dit.

The reason I'm asking this question— and I don't mean to pick on Germany here, but obviously you have spent a lot of time in Germany and in this space— is if a German bank was attacked and a Canadian bank was attacked and if the German bank and the Canadian bank went on the offence, who would win? Who would be better prepared to deal with cybersecurity threats? Would it be the German bank or the Canadian bank, or do you know?

Si je pose cette question — et loin de moi l'idée de m'acharner sur l'Allemagne, mais de toute évidence, vous y avez passé beaucoup de temps —, c'est que si une banque allemande et une banque canadienne étaient la cible d'une attaque et que les deux passaient à l'offensive, laquelle gagnerait? Laquelle des deux banques est mieux préparée à faire face à des menaces à la cybersécurité? Le savez-vous?

**Mr. Kerschbaum:** I think the banks we are dealing with in Canada are reasonably well prepared to take the topic seriously; so are the German banks. I think they would probably be on a comparable level. If one went to attack and the other one went to attack, I think we would be in a nuclear war and both would lose.

**M. Kerschbaum :** Je pense que les banques canadiennes sont assez bien préparées à prendre la chose au sérieux; et il en est de même pour les banques allemandes. Ce serait probablement comparable. Si les deux passaient à l'attaque, je crois que nous entrerions dans une guerre nucléaire et que les deux perdraient.

**Senator Wetston:** That's reassuring. Thank you.

**Le sénateur Wetston :** C'est rassurant. Merci.

**Senator MacDonald:** It's great to have you here today professor. Like a lot of people my age, I love technology but I don't always understand it. I use it as much as I can, but security seems to be a concern of everybody now, particularly when you are not well versed and you are a little blinded by it and need some direction. You mention here that customers do not pay for security, but I would think the government should.

**Le sénateur MacDonald :** C'est formidable de vous accueillir, monsieur. Comme bien des gens de mon âge, j'aime la technologie, mais je ne la comprends pas toujours. Je l'utilise le plus possible, mais il semble que la sécurité préoccupe tout le monde maintenant, surtout si l'on ne s'y connaît pas bien, que la technologie nous aveugle un peu et qu'on a besoin d'orientation. Vous dites que les clients ne paient pas pour la sécurité, mais à mon avis, le gouvernement devrait le faire.

We always use BlackBerries around here. I was in the States a few years ago, in a congressman's office. They had just come back from a trip to China and they were told not to take their iPhones and put them away. The only thing they were able to use was their old BlackBerries, which they dug out and took with them. In Ottawa in the last few years we've been given permission to use iPhones. A lot of people are getting away from BlackBerries but I'm not. I'm still with BlackBerry.

Nous utilisons encore des BlackBerry. Il y a quelques années, j'étais dans le bureau d'un membre du Congrès américain. Il revenait d'un voyage en Chine et on avait dit aux gens de ne pas utiliser leur iPhone. La seule chose qu'ils pouvaient utiliser, c'était leurs vieux BlackBerry, qu'ils ont ressortis et apportés. À Ottawa, on nous permet d'utiliser des iPhone depuis quelques années. Bon nombre de gens abandonnent leur BlackBerry, mais ce n'est pas mon cas. J'utilise encore le mien.

Could you comment on this? Is the Government of Canada being maybe a little reckless or sloppy, or is it there is nothing to be concerned about when it comes to the devices we use for communicating?

**Mr. Kerschbaum:** I think if you are in a responsible role, you have to be very careful. I will use Germany as an example again. Of course, it went to the German news that the NSA was tracking Angela Merkel's phone. She didn't use the phone built by the German government for that and they were tracking that phone number.

One must understand there will never be 100 per cent security. However, we also have to understand that we have to care for our security which goes back to the first question. We have to accept some inconvenience like using a BlackBerry instead of an iPhone. There should definitely be some best practices. I believe for members of the government there should be some recommendations about what device you are supposed to use for what purpose, as it was, for example, in the Angela Merkel case.

**Senator MacDonald:** I want to make sure. The China technology firm Huawei is a huge company and there are concerns about them purchasing high-tech companies in Canada and the United States. The U.S. security people are extremely concerned about it and said that the government should be concerned, yet the response of the Government of Canada is that we should not be concerned. Who would you side with, the U.S. or the Canadian government when it comes to assessing this threat?

**Mr. Kerschbaum:** Again, it is a difficult question. I'm not inside the company Huawei. I know that the company makes a lot of efforts trying to enhance the security of their products. However, their main development still remains in China. I would assume some intelligence agency has some idea of what is going on in China and I would trust that report.

**Senator Marwah:** Thank you, Mr. Kerschbaum, for your comments.

First of all, I would like to congratulate the University of Waterloo on their newly established Cybersecurity and Privacy Institute. I think that's fantastic and they have always been on the leading front of IT.

In your comments, you suggested one of the ways to really make progress or deal with the issue of cybersecurity was incentives. Could you elaborate on what you mean by "incentives" and who should be providing the incentives?

Pourriez-vous nous donner votre point de vue là-dessus? Se peut-il que le gouvernement du Canada soit un peu imprudent ou négligent, ou bien c'est parce qu'il n'y a pas lieu de s'inquiéter lorsqu'il s'agit des appareils que nous utilisons pour communiquer?

**M. Kerschbaum :** Je pense que toute personne qui joue un rôle de responsable doit être très prudente. Je vais prendre l'exemple de l'Allemagne encore une fois. Bien sûr, on a appris dans les nouvelles au pays que la NSA avait mis sur écoute le téléphone d'Angela Merkel. Elle n'utilisait pas le téléphone fourni par le gouvernement allemand pour cela et ce numéro de téléphone était suivi.

Il faut comprendre que ce ne sera jamais sécuritaire à 100 p. 100. Toutefois, nous devons également comprendre qu'il nous faut nous soucier de notre sécurité, ce qui nous ramène à la première question. Nous devons accepter certains désagréments, comme utiliser un BlackBerry plutôt qu'un iPhone. Assurément, des pratiques exemplaires devraient être suivies. Je crois qu'on devrait faire des recommandations aux membres du gouvernement quant aux appareils qu'ils sont censés utiliser selon le but, comme dans le cas d'Angela Merkel.

**Le sénateur MacDonald :** Je veux m'assurer d'une chose. L'entreprise de technologie chinoise Huawei est énorme et l'on craint qu'elle achète des entreprises de haute technologie canadiennes et américaines. Aux États-Unis, les responsables de la sécurité sont extrêmement préoccupés à cet égard et ils ont dit que le gouvernement devrait être inquiet; pourtant le gouvernement du Canada a dit que nous ne devrions pas nous inquiéter. De quel côté vous rangez-vous dans l'évaluation de cette menace? Êtes-vous du même avis que le gouvernement américain ou le gouvernement canadien?

**M. Kerschbaum :** Encore une fois, c'est une question difficile. Je ne fais pas partie de l'entreprise Huawei. Je sais qu'elle consacre beaucoup d'efforts à améliorer la sécurité de ses produits. Toutefois, ses principaux projets sont réalisés en Chine. J'imagine qu'un organisme de renseignement aurait une idée de ce qui se passe en Chine, et j'aurais confiance en cet avis.

**Le sénateur Marwah :** Monsieur Kerschbaum, je vous remercie de vos observations.

J'aimerais tout d'abord féliciter l'Université de Waterloo pour l'Institut de la cybersécurité et de la protection des renseignements personnels qu'elle a établi récemment. C'est formidable. Elle a toujours joué un rôle de premier plan dans les TI.

Dans vos remarques, vous avez dit qu'un des moyens de faire de vrais progrès ou de s'attaquer aux défis de la cybersécurité, c'est d'offrir des incitatifs. Pourriez-vous nous expliquer ce que vous entendez par « incitatifs » et nous dire qui devraient les offrir?

**Mr. Kerschbaum:** That's a very good question. As a company, I have to make some profit, so I will build a product that maximizes my profit. Now, if bad cybersecurity doesn't impact my profit but only appears as a cost, then I will invest less in cybersecurity. So it starts with the awareness of the users that do not select products.

We had the question: If you could choose between an iPhone and a BlackBerry, and you knew that the BlackBerry would be more secure, if you weren't told to use the BlackBerry, would you use it or would you rather go with the iPhone? So in your consideration, you're not taking into account the security aspect, but naturally most people would go with the more modern phone, the iPhone. As a company, of course, I have to adjust to this. Now I will build the faster, nicer, better-looking phone with more features and thereby not pay as much attention to cybersecurity.

However, if you look at this from a Canadian perspective, then this is, of course, bad because vital data or data of Canadians might be broken, abused. And therefore, it is very difficult. I don't want to necessarily propose a solution but these centres of excellence in the U.S. or these research programs or these investments in cybersecurity that are being made, in my opinion, are a response to what I would almost call a market failure in cybersecurity. And therefore, the question is, as a nation or a government, how do we respond to this market failure in some sense?

Maybe we can deal with education and get people more interested in security. Maybe it fixes itself over time. I would not predict that, but we see that other governments are investing in cybersecurity and they take the bill for industry in some sense.

I would assume that this will put some pressure on Canada in the long run. As with the bear, one has to at least out run the competitor.

**Senator Marwah:** I'm still confused about where the word "incentives" comes in. Incentives to whom? Are you referring to tax incentives? What incentives are you referring to?

**Mr. Kerschbaum:** I mean the incentives in an economic sense, to maximize your profit. If you want to maximize your profit, you do not invest as much to achieve a high level of security. The incentives for a company are on spending money somewhere other than security.

**Senator Wallin:** I have a follow-up related to Senator Marwah's question about your comments that customers don't pay for security. So whose role is it to do that? Because it's a

**M. Kerschbaum :** C'est une très bonne question. Puisqu'une entreprise doit faire des profits, elle doit concevoir un produit qui permet de les maximiser. Maintenant, si de mauvaises pratiques en matière de cybersécurité n'ont pas de répercussions sur ses profits et ne figurent que parmi les dépenses, alors l'entreprise investira moins dans la cybersécurité. Cela commence donc par une prise de conscience chez les utilisateurs qui ne choisissent pas des produits.

Nous avions la question suivante : si vous aviez le choix entre un iPhone et un BlackBerry, et que vous saviez que le BlackBerry est plus sécuritaire, si on ne vous disait pas d'utiliser le BlackBerry, l'utiliseriez-vous ou opteriez-vous plutôt pour le iPhone? Donc, dans la réflexion, on ne tient pas compte de l'aspect sécuritaire, mais naturellement, la plupart des gens choisiraient le téléphone le plus récent, soit le iPhone. Bien entendu, une entreprise doit s'adapter. Elle se dit qu'elle va maintenant fabriquer un téléphone plus rapide et plus beau qui inclut plus de fonctions et, de ce fait, elle n'accordera pas beaucoup d'attention à la cybersécurité.

Cependant, si l'on regarde les choses d'un point de vue canadien, alors bien entendu, c'est déplorable, car des données cruciales ou les données de Canadiens pourraient être utilisées de façon abusive. Par conséquent, c'est très difficile. Je ne veux pas nécessairement proposer une solution, mais à mon avis, les centres d'excellence aux États-Unis, les programmes de recherche ou les investissements en cybersécurité constituent une réponse à ce que j'appellerais presque un échec du marché en cybersécurité. C'est pourquoi la question qui se pose est la suivante : que doivent faire une nation ou un gouvernement devant cet échec du marché en un sens?

Nous pourrions axer nos efforts sur l'information et amener les gens à s'intéresser davantage aux questions de sécurité. Peut-être que les choses s'arrangeront au fil du temps. Je ne le prédirais pas, mais nous voyons que d'autres gouvernements investissent dans la cybersécurité et paient la facture pour l'industrie en quelque sorte.

Je suppose qu'à long terme cela mettra de la pression sur le Canada. Il faut du moins distancer les concurrents.

**Le sénateur Marwah :** Je ne comprends toujours pas ce que vous entendez par « incitatifs ». Des incitatifs pour qui? Parlez-vous d'incitatifs fiscaux? De quoi s'agit-il?

**M. Kerschbaum :** Je parle d'incitatifs au sens économique, de la maximisation des profits. Si l'on veut maximiser les profits, on n'investit pas beaucoup d'argent pour atteindre un niveau de sécurité élevé. Pour une entreprise, il s'agit d'investir de l'argent dans d'autres volets que celui de la sécurité.

**La sénatrice Wallin :** J'ai une question liée à celle du sénateur Marwah qui porte sur votre observation selon laquelle les clients ne paient pas pour la sécurité. À qui appartient-il de le

given, it's a must and it's necessary, so if you believe it's government's role to do that, in our particular case, then we have privacy issues. We have competence issues. We have funding issues.

We have big data operators that are much bigger than our governments, so what's that next step? You've made the case that customers won't pay and businesses aren't incented to do it, so where does it fall?

**Mr. Kerschbaum:** I do think it falls towards the government. There is a need to invest in more cybersecurity, be it in a combination of agencies, in programs to enhance cybersecurity and, of course, for research and education. It is difficult for fundamental cybersecurity researchers to get industry funding. If you have a project that's very well advanced and is the state of the art where you have an idea that it is high-risk and might leapfrog some of the problems we have, it can be very difficult to find someone willing to partner with you. And then you have to go with more competitive funding programs, whereas my German colleagues can go to the same company and can say, "I have enough money, I will do it for you for free," and they can work on it.

**Senator Wallin:** That does raise the question. We're watching the crisis — I don't know how else to call it — with big data, Facebook and everything within the last 48 hours, but it's every day, so they do have the money. Would you envision a tax on these? Government doesn't have money to pay for this kind of research. It's a huge, expensive venture. Do you get the money from those guys or how do you see this happening?

**Mr. Kerschbaum:** I'm not an expert on how to implement this, and I do not necessarily want to impose something but if you spend money you have to collect money.

**Senator Tkachuk:** I had a number of questions. To go back to what you talked about in the early part of your presentation about the skills needed for cybersecurity, what are the necessary skills at the high school level? What should students be studying if they are interested in this field and what are the best areas to study if they're interested in this field?

**Mr. Kerschbaum:** That is a very good question. I think cybersecurity as a field is too early for high school. Usually education starts after you have learned basic programming skills, basic skills in understanding how a computer system works and only then can you dive into the specific aspects of becoming a cybersecurity professional.

faire? Puisque cela va de soi et que c'est indispensable, si l'on croit qu'il appartient au gouvernement de le faire, dans notre cas, il y a des questions liées à la protection des renseignements personnels, aux compétences et au financement qui entrent en jeu.

Puisqu'il y a des opérateurs de mégadonnées qui sont beaucoup plus grands que nos gouvernements, alors quelle est la prochaine étape? Vous dites que les clients ne paieront pas et que rien n'encourage les entreprises à cet égard. De qui cela relève-t-il?

**M. Kerschbaum :** Je crois qu'il appartient au gouvernement de le faire. Il faut investir davantage dans la cybersécurité, qu'il s'agisse d'un ensemble d'organismes, de programmes visant à améliorer la cybersécurité ou, bien entendu, de la recherche et de l'éducation. Dans la recherche fondamentale, il est difficile pour les chercheurs en cybersécurité d'obtenir du financement. Si un projet va vraiment bon train et qu'il est ultramoderne, qu'on a une idée qui présente un risque élevé et qui pourrait permettre de surmonter une partie des problèmes que nous avons, il peut être très difficile de trouver quelqu'un qui est prêt à s'associer au projet. Ensuite, il faut opter pour des programmes de financement plus concurrentiels, tandis que mes collègues allemands peuvent s'adresser à la même entreprise et dire : « J'ai assez d'argent; je vais le faire pour vous gratuitement », et ils peuvent y travailler.

**La sénatrice Wallin :** Il y a donc lieu de poser la question. Nous voyons actuellement la crise — j'ignore quel autre nom donner à cette situation — sur les mégadonnées, Facebook et tout ce qui s'est passé au cours des deux derniers jours, mais puisque c'est tous les jours, ils ont l'argent. Croyez-vous qu'une taxe pourrait être imposée? Le gouvernement n'a pas l'argent qu'il faut pour payer pour ce type de recherche. C'est une énorme entreprise qui est très coûteuse. Obtient-on l'argent de ces gens-là? Comment cela fonctionnerait-il, selon vous?

**M. Kerschbaum :** Je ne suis pas un spécialiste quant à la façon de mettre cela en œuvre, et je ne veux pas nécessairement qu'on impose quelque chose, mais si l'on dépense de l'argent, il faut en amasser.

**Le sénateur Tkachuk :** J'avais un certain nombre de questions. Pour revenir à ce que vous disiez dans la première partie de votre exposé au sujet des compétences requises en matière de cybersécurité, quelles sont les compétences nécessaires au niveau de l'école secondaire? Quelle matière les élèves doivent-ils étudier si le domaine les intéresse et quels sont les meilleurs domaines d'étude?

**M. Kerschbaum :** C'est une très bonne question. Je crois qu'au secondaire, il est trop tôt pour étudier la cybersécurité. Habituellement, cela commence après l'acquisition de compétences de base, l'apprentissage du fonctionnement d'un système informatique. C'est seulement par la suite qu'on plonge

However, there is awareness for security where you understand a need for security, that you have to protect your private data, that you decide what you share with Facebook and if you decide what you share, what that means and implies to your data. These kinds of decisions need to be understood, probably even earlier than high school.

**Senator Tkachuk:** Do they need to know math, physics, what skill level? To be a computer scientist, what do you need to be good at?

**Mr. Kerschbaum:** It's basically a combination of math and engineering.

**Senator Tkachuk:** Physics, geometry, all that stuff? What would you say are the most vulnerable areas in our country to cyberattacks and what are the most dangerous areas to cyberattacks, if you were going to rank one, two, three, four.

**Mr. Kerschbaum:** That is a very good question. When new products are being developed and deployed for innovation using computers, they usually are deployed with insufficient consideration for security. So if we're now moving into IOT cities, cities that have sensors and actuators everywhere, I think that there would be a huge risk. With this whole field of Internet of Things, I would rank by far number one.

Most of the IOT devices by now do not have sufficient cybersecurity and we do not understand what the implications of a lot of aspects of cybersecurity will be.

The impacts are huge because they often impact on physical things, whereas if I break into a bank and a lot of money gets lost, I'm probably able to recover bits and bytes somehow. However, if somebody dies, that's permanent.

**Senator Tkachuk:** Okay. So the whole technology of driverless vehicles, if what they are talking about is true and what they are trying to do is true, it would seem to be fairly easy to gum up the whole system.

**Mr. Kerschbaum:** Yes, it probably will be. Even the technologies used, if we think about the machine learning technologies that are underneath this — because I try to sort of understand the world around me in a probabilistic way, in some senses. I try to interpret, does this look like a stop sign? And there are ways of tricking an algorithm that tries to detect a stop sign but will see a speed limit sign. Then problems arise.

dans les aspects précis qui permettront à quelqu'un de devenir un professionnel de la cybersécurité.

Toutefois, il y a la notion de conscience concernant la sécurité. Il s'agit de comprendre qu'il y a un besoin en matière de sécurité, qu'il faut protéger ses renseignements personnels; une personne décide ce qu'elle partage sur Facebook, et si elle le fait, elle doit comprendre ce que cela signifie pour ses données. Ces décisions doivent être bien comprises, probablement même avant l'école secondaire.

**Le sénateur Tkachuk :** Doit-on être bon en mathématiques et en physique? Dans quelle matière faut-il être doué pour devenir informaticien?

**M. Kerschbaum :** Il s'agit essentiellement d'une combinaison de mathématiques et de génie.

**Le sénateur Tkachuk :** La physique, la géométrie et ainsi de suite? À votre avis, quels sont les secteurs les plus vulnérables aux cyberattaques dans notre pays et quels sont les secteurs les plus dangereux pour les cyberattaques, si vous deviez établir un ordre?

**M. Kerschbaum :** C'est une très bonne question. Lorsque de nouveaux produits sont conçus et déployés pour l'innovation et qu'on utilise des ordinateurs, ils sont habituellement déployés au détriment de la sécurité. Si l'on utilise l'Internet des objets pour les villes, c'est-à-dire qu'il y aurait des capteurs et des actionneurs partout, je pense que cela poserait d'énormes risques. Le domaine de l'Internet des objets est de loin au premier rang de mon classement.

À l'heure actuelle, la plupart des appareils de l'Internet des objets ne conviennent pas sur le plan de la cybersécurité et nous ne savons pas quelles incidences auront bon nombre d'aspects de la cybersécurité.

Les répercussions sont énormes, car il y a souvent des effets sur des choses concrètes, tandis que si j'entre par effraction dans une banque et qu'on perd beaucoup d'argent, je vais probablement être en mesure de récupérer des bits et des octets en quelque sorte. Cependant, si quelqu'un meurt, c'est permanent.

**Le sénateur Tkachuk :** D'accord. Donc, pour ce qui est de la technologie des véhicules autonomes, si ce qui est dit est vrai et si ce qu'on essaie de faire est vrai, il me semble qu'il serait assez facile de bousiller tout le système.

**M. Kerschbaum :** Oui, ce sera probablement le cas. Même les technologies utilisées, si nous pensons aux technologies d'apprentissage machine — parce que j'essaie en quelque sorte de comprendre le monde qui m'entoure selon un point de vue probabiliste, dans certains cas. J'essaie de déterminer si telle affiche ressemble à un panneau d'arrêt. Et il existe des façons de tromper un algorithme qui essaie de détecter un panneau d'arrêt,

Particularly if I determine the future threat to computer systems, if we talk about research, then this whole field of machine learning, security and privacy we have not understood at all.

**Senator Tkachuk:** I have one more question. You talked earlier about companies not having enough incentive or there wasn't proper incentive because the stock market didn't sort of react to cybersecurity or a problem. I'm not sure whether Facebook gave away the information, the information was stolen, it was sold by someone inside the system or sold to the profit of the company. Nonetheless, its revelation has caused huge penalties for Facebook on the stock market right now. I don't know eventually how long that will last. Nonetheless, there was an immediate reaction.

Don't you think a huge problem, say, in CIBC would cause exactly the same thing? I mean, wouldn't it be devastating to them if there were tons of accounts revealed through a cyberattack? Because that means people can get into them, I would think.

**Mr. Kerschbaum:** I certainly assume that it would be newsworthy and that we would hear about it. However, think about when you decide which bank to use. Is your number one decision that I'm going to switch my bank now because my accounts are broken, my balances are the same, so I don't really feel a monetary impact? If they would lose your balance and not be able to recover it, then you would certainly switch.

**The Chair:** It's too late.

**Mr. Kerschbaum:** Then it's too late, yes, but if you don't feel an impact and just your data was stolen, would that be sufficient for you to say, "I will walk 500 metres more to the next ATM"? I am not so sure.

**Senator Tkachuk:** It would depend. If there were dozens and dozens of accounts that were stolen, you're darn right I'd be interested in getting my money out of that bank. I think most people would.

**Senator Ringuette:** On another issue, we heard in this committee about hackers being used, and so far we have not talked about the attackers. We're assuming that a lot of these hackers don't have an engineering or computer science degree. Some of them are very young, smart and keen and are able to think outside of the box as you were talking about.

How much effort are we putting into recruiting these inquisitive minds?

mais qui verra un panneau indiquant la limite de vitesse. C'est alors que des problèmes surviennent. En particulier, si je détermine la future menace pour les systèmes informatiques, si nous parlons de recherche, alors nous n'avons pas compris du tout ce domaine d'apprentissage machine, de sécurité et de vie privée.

**Le sénateur Tkachuk :** J'ai une autre question. Vous avez dit plus tôt qu'il y a un manque d'incitatifs ou de bons incitatifs parce que le marché des valeurs mobilières n'a pas réagi en quelque sorte à la cybersécurité ou à un problème. Je ne sais pas si Facebook a divulgué l'information, si l'information a été volée, si elle est a été vendue par quelqu'un dans le système ou vendue au profit de l'entreprise. Néanmoins, cela a énormément pénalisé Facebook dans le marché des valeurs mobilières. Je ne sais pas combien de temps la situation durera. Néanmoins, il y a eu une réaction immédiate.

Ne pensez-vous pas qu'un énorme problème, chez CIBC, disons, causerait exactement la même situation? Ne serait-il pas catastrophique pour elle si des tonnes de comptes étaient touchés par une cyberattaque? Cela voudrait dire que les gens peuvent y accéder, à mon avis.

**M. Kerschbaum :** Je présume que cela ferait les manchettes et que nous en entendrions parler. Toutefois, pensez au moment où vous décidez avec quelle banque vous ferez affaire. Est-ce que vous décidez en premier lieu de changer de banque maintenant parce que vos comptes ont été touchés, mais votre solde est le même et il n'y a pas vraiment de conséquences financières? Si la banque perd votre solde et n'est pas capable de le récupérer, alors vous changeriez assurément de banque.

**Le président :** C'est trop tard.

**M. Kerschbaum :** C'est trop tard, oui, mais à moins d'en sentir les conséquences, est-ce que le vol de vos données suffira pour vous convaincre de faire 500 mètres de plus jusqu'au prochain guichet? Je n'en suis pas certain.

**Le sénateur Tkachuk :** Tout dépend de la situation. Si des dizaines et des dizaines de comptes avaient été piratés, vous pouvez être certain que je voudrais sortir mon argent de cette banque. Je crois que c'est ce que feraient la plupart des gens.

**La sénatrice Ringuette :** Dans un autre ordre d'idées, des témoins ont dit au comité que des pirates servent de pions à ceux qui orchestrent de telles attaques. Jusqu'à maintenant, nous n'avons pas parlé de ces chefs d'orchestre. Je présume que bon nombre de ces pirates ne sont ni ingénieurs ni informaticiens. Certains sont très jeunes; ils sont intelligents, astucieux et créatifs, comme vous le mentionniez.

À quel point multiplie-t-on les efforts pour recruter ces grands esprits?

**Mr. Kerschbaum:** There is research and there is an opinion in a large part of the research community on this.

First of all, if you want to become a security professional, you have to have a high standard of ethics. So it is actually very much frowned upon to hire former Black Hat Hackers as security professionals. You have to be very careful. You have to imagine that you're dealing with someone who might well have attacked you before. Now that he is an insider, how do you know he is not going to attack you from the inside?

**Senator Ringuette:** No, I'm talking about for research purposes. They know how to break into systems, so they should know how to eliminate the potential of breaking into systems.

**Mr. Kerschbaum:** Now, there is another piece of research on which there is an assumption that if you are actually skilled at computer sciences and hacking, you work for the good guys. There is also a somewhat hand-waving analysis that if you are not that skilled, it pays for you to be an attacker. So I would assume the skilled people are actually working on the defence or on the good side and you don't have to become a criminal if you can actually make a living without that.

How to get into the situation again might be one of education, but it is not likely that we have the attackers — I have a train of thought here. The reason why we still see attacks from people who presumably are not as skilled as the defenders is my first point, where I said that cyberdefence is so much more difficult than cyberoffence. It is relatively easy to take a new product like an IOT product and make a class with people who have never done cybersecurity and have them break into these products. I would assume that 10 out of 10 students would be successful if you gave them a little background. However, teaching someone to develop an IOT product able to withstand these attacks, you might need to go to the PhD level.

**The Chair:** Before we move to the second round, I have a couple of questions arising from what my colleagues have raised with you.

I took from what you said that your fair opinion is the state of research in cybersecurity in Canada would not be as high as other G7 countries. Canada is lagging in research in cybersecurity, I heard you just say.

**Mr. Kerschbaum:** Definitely compared to the top in the G7.

**The Chair:** Thank you very much. So let's look at the U.S., for example, which you mentioned on a couple of occasions. When we talk about these centres of excellence in the U.S., are they affiliated with universities? Are they funded by industry? Help us understand the structure, please, of those organizations.

**M. Kerschbaum :** Des recherches sont faites à ce sujet, et les chercheurs s'entendent généralement là-dessus.

D'abord, pour devenir un professionnel de la sécurité, il faut posséder un grand sens de l'éthique. C'est donc très mal vu d'embaucher d'anciens chapeaux noirs à titre d'experts en sécurité. Il faut être très prudent. Il n'est pas impossible que vous ayez affaire à quelqu'un qui vous a piraté auparavant. Si vous lui donnez accès au réseau interne, comment savoir qu'il ne vous attaquera pas de l'intérieur?

**La sénatrice Ringuette :** Non, je veux dire à des fins de recherche. Ils savent comment s'introduire frauduleusement dans les systèmes, alors ils devraient savoir comment éliminer les risques d'introduction.

**M. Kerschbaum :** On peut présumer que les plus doués travaillent du bon côté, et qu'il est plus payant pour les autres de se tourner vers le piratage. C'est une analyse quelque peu simpliste de la chose, mais j'imagine que les gens compétents travaillent à la défense ou du bon côté, et qu'il n'est pas nécessaire d'être un criminel pour bien gagner sa vie.

L'éducation pourrait être une piste de solution, mais il est peu probable que nous recrutions les pirates. Vous allez comprendre ma logique. Si nous devons encore contrer des attaques de la part de pirates qui sont moins compétents que les experts en sécurité, c'est qu'il est beaucoup plus difficile d'assurer une cyberdéfense que de perpétrer une cyberattaque, d'où mon premier argument. Il est relativement facile d'enseigner à des non-initiés comment pirater un nouveau produit, par exemple un produit de l'Internet des objets (IdO). Je dirais que 10 élèves sur 10 réussiraient si on leur donnait un peu d'information. Cependant, pour enseigner à quelqu'un comment développer un produit de l'IdO qui pourrait résister à de telles attaques, il faudrait sans doute se rendre au doctorat.

**Le président :** Avant de passer au deuxième tour, j'aimerais revenir sur quelques-unes des questions posées par mes collègues.

D'après vos commentaires, j'en conclus que la recherche en matière de cybersécurité au Canada accuse un certain retard par rapport à d'autres pays du G7. Le Canada traîne un peu derrière, si je vous ai bien compris.

**M. Kerschbaum :** Par comparaison aux premiers pays du G7, certainement.

**Le président :** Merci beaucoup. Prenons les États-Unis, par exemple, que vous avez mentionnés à quelques reprises. Les centres d'excellence américains sont-ils affiliés à des universités? Sont-ils financés par l'industrie? Aidez-nous à comprendre la structure de ces organisations, s'il vous plaît.

**Mr. Kerschbaum:** So these are mostly funded by the government. The government has established centres of excellence that have a clear educational purpose to educate mostly master's students in cybersecurity and help fund scholarships and professorships in the universities.

Now, there are also funding programs, like from IARPA, for specific cybersecurity technologies. These are open to companies as well, so companies can apply for these, but often universities and companies collaborate.

**The Chair:** Could you refer us to the names of a couple of institutes in the U.S., these centres of excellence, either now or subsequently?

**Mr. Kerschbaum:** I'm a graduate of the Purdue University, which has the CERIAS institute, and that's part of NSA Centres of Excellence.

**The Chair:** Thank you very much. They have a good basketball team too.

**Mr. Kerschbaum:** Didn't they lose?

**The Chair:** They lost, but it's still a good team. Okay, thank you very much for that.

Given that Waterloo has the germination, the 40 professionals that you have, could that be enhanced to be a centre of excellence in Canada, and, if so, what would it take to do that?

**Mr. Kerschbaum:** I think it could, and I think it will take some time and dedication at the University of Waterloo. It might need some additional money for scholarships to attract people, to attract good students to that program and to perhaps fund a couple of specialized additional professorships.

**The Chair:** Thank you very much. You mentioned something in your comment. I think you called it IRAP or IPAC or something. When I was asking about centres of excellence, you said that there's a granting program in the U.S. called —

**Mr. Kerschbaum:** IARPA.

**The Chair:** I would like to ensure that our analysts have that so that we can see what they are doing.

Last question, if I can: If you are able to, how does the German state work with business on these issues, if you know?

**M. Kerschbaum :** Ils sont majoritairement financés par le gouvernement. Le gouvernement a établi des centres d'excellence à vocation académique, qui visent principalement les étudiants à la maîtrise en cybersécurité; l'objectif est aussi de contribuer au financement de bourses d'études et de chaires d'enseignement dans les universités.

Il y a également des programmes de financement, comme l'IARPA, qui sont voués précisément aux technologies de cybersécurité. Ces programmes sont aussi ouverts aux entreprises, mais on voit souvent des projets menés conjointement par les universités et l'industrie.

**Le président :** Pourriez-vous nous donner le nom de quelques instituts ou centres de recherche aux États-Unis? Ce peut-être maintenant ou plus tard.

**M. Kerschbaum :** Je suis diplômé de l'Université Purdue, où est situé l'institut CERIAS, qui fait partie du réseau de centres d'excellence de la NSA.

**Le président :** Merci beaucoup. Elle a d'ailleurs une bonne équipe de basketball.

**M. Kerschbaum :** N'a-t-elle pas perdu?

**Le président :** Elle a perdu, mais cela reste une bonne équipe. Très bien, merci pour votre réponse.

Puisqu'il y a cet incubateur à Waterloo — je parle des 40 professionnels qui travaillent avec vous —, pourrait-on aller plus loin et en faire un centre d'excellence pour le Canada? Que faudrait-il pour concrétiser ce projet?

**M. Kerschbaum :** Je crois que oui, et je crois que cela prendra du temps et de l'engagement de la part de l'Université de Waterloo. Il faudrait sans doute prévoir des fonds supplémentaires afin d'offrir des bourses d'études pour attirer des étudiants de talent; et peut-être financer quelques chaires d'enseignement spécialisé supplémentaires.

**Le président :** Merci beaucoup. Vous avez parlé de l'IRAP ou de l'IPAC, ou quelque chose comme cela. En parlant des centres d'excellence, vous avez dit qu'il y a un programme de subventions aux États-Unis appelé…

**M. Kerschbaum :** L'IARPA.

**Le président :** Je veux m'assurer que nos analystes ont pu le noter correctement, car nous allons vouloir en savoir plus là-dessus.

Une dernière question, si vous le voulez bien. Savez-vous de quelle manière l'État allemand travaille avec l'industrie dans ce domaine?

**Mr. Kerschbaum:** I only know to a small degree, but one of the tasks of German BSI is to give recommendations to companies to evaluate and to have a standard of security. If you want to sell to the government or want to get a seal of approval, you have to meet certain security standards. These are documented. These are updated regularly, and they are something one can refer to.

**The Chair:** Thank you very much. It's very helpful.

**Senator Ringuette:** To further that line of discussion, the ISO certification recognized worldwide, would they be working on a similar certification of cybersecurity for industry?

**Mr. Kerschbaum:** There are some efforts on, for example, what is called a "software-development lifecycle" I'm aware of. There are some efforts for certain mechanisms. However, in what the ISO does, its processes, there are what I would call parameters to that process, like some technical things. I will just give you an example: How long does a cryptographic key have to be? That essentially changes over time. So you have to have both. You have to have a process, and you have to have the parameters. At a European level, there is also, for example, the ENISA Institute, which also, issues some of those recommendations from time to time on these parameters that you are supposed to employ.

**Senator Ringuette:** There is work being done at that international level.

**Mr. Kerschbaum:** There is definitely at the international level, yes.

**Senator Wetston:** I have a quick follow-up on the educational part. I'm pretty persuaded that science is important, and I'm also persuaded that our world is being run more and more by technology and technological advance. I think we can all agree with that. I hear, from your testimony here, you are more or less making recommendations to this Senate committee, which it, obviously, would consider in its report, but what I'm wondering about is: You've probably been in Canada long enough to appreciate the fact that we have under invested in STEM programs in Canada, and there have been some efforts recently to try to encourage greater education initiatives around STEM programs, which I think is probably essential. I'm not sure whether you agree with that or not, but I suspect you would.

Can you tell me whether or not you believe that advancement in STEM programs would be of some benefit because it could lead to potentially having students and scientists with greater capability in cybersecurity, and would that be a recommendation of yours as well?

**M. Kerschbaum :** Je ne le sais pas exactement, mais je peux vous dire qu'une des fonctions du BSI, en Allemagne, est de formuler des recommandations à l'intention des entreprises et d'établir des normes de sécurité. Pour conclure un contrat de vente avec le gouvernement, ou pour obtenir un sceau d'approbation, les entreprises doivent satisfaire à différents critères de sécurité. Le tout est documenté. Les normes sont mises à jour régulièrement et il est possible de les consulter.

**Le président :** Merci beaucoup. C'est très intéressant.

**La sénatrice Ringuette :** Pour poursuivre dans la même veine, la certification ISO est reconnue mondialement; est-ce qu'on travaille à une certification semblable pour l'industrie en matière de cybersécurité?

**M. Kerschbaum :** À ma connaissance, il y a certains efforts déployés notamment en vue de mettre en œuvre une plateforme de gestion du cycle de vie du développement des logiciels. On travaille à la mise en place de quelques mécanismes. Cependant, pour ce qui est de la certification ISO, il y a des paramètres techniques qui se rattachent au processus, si je peux m'exprimer ainsi. Je peux vous donner un exemple : combien de symboles doit contenir une clé cryptographique? Ces paramètres changent au fil du temps. Alors les deux sont nécessaires : le processus et les paramètres. En Europe, il y a aussi l'institut ENISA, qui émet sporadiquement des recommandations concernant les paramètres à appliquer.

**La sénatrice Ringuette :** Il y a des efforts qui sont faits en ce sens à l'échelle internationale.

**M. Kerschbaum :** À l'échelle internationale, tout à fait, oui.

**Le sénateur Wetston :** J'aimerais revenir brièvement sur le volet éducation. Je suis persuadé que la science est importante, et je suis aussi persuadé que notre monde est de plus en plus mené par la technologie et les avancées technologiques. Je crois que nous sommes tous d'accord là-dessus. Témoigner devant notre comité sénatorial revient ni plus ni moins à nous faire des recommandations, dont nous allons évidemment tenir compte pour produire notre rapport. Voici la question que je me pose : vous êtes probablement ici depuis assez longtemps pour savoir que nous avons sous-financé les programmes de sciences, technologies, génie, mathématiques et sciences informatiques au Canada. Récemment, des efforts ont été déployés afin d'encourager l'élaboration de plus d'initiatives d'enseignement liées à ces matières, et c'est sans doute essentiel. Êtes-vous aussi de cet avis? Je présume que oui.

Pensez-vous que favoriser ces matières pourrait être une bonne chose, puisque cela pourrait se traduire par un bassin d'étudiants et de chercheurs mieux ferrés sur la cybersécurité? Serait-ce aussi votre recommandation?

**Mr. Kerschbaum:** Absolutely.

**Senator Wetston:** Any thoughts on how you might make that happen?

**Mr. Kerschbaum:** It is a little bit outside of my area of expertise, but let me talk from my personal experience. When I was in high school in Germany, there was no computer science subject. Now, there is a computer science subject that you can take at the higher level of high school. That's a very good advance. I also think in a lot of cases, this awareness of things, how to deal with these types of technologies, is a very important aspect and data security and privacy should be one of the important aspects.

Of course, a computer is fundamentally a mathematical object, and the more math you understand, the easier it is to understand a computer.

**Senator Wetston:** So the corporate sector, particularly large public companies and not just in financial services, if you look at large forums like the World Economic Forum, when they meet and present their global view, whether it's business or other areas, invariably, the CEOs of these international, global public companies would list cybersecurity as one of the major threats to their companies, whether it's IP or data or financial services or climate change, which isn't very high on the list as well. If that is the case, are you suggesting that, possibly, we're not taking it seriously enough to invest in the education side, to invest in security, whether it be at the government level or at the corporate level? Is that your suggestion?

**Mr. Kerschbaum:** Yes, it is. It's interesting you mention climate change, which is caused by pollution, as one of the big threats. Of course, without regulation, companies wouldn't do much in order to prevent pollution. There might be an analogy to cybersecurity here.

**The Chair:** Very interesting.

**Senator Unger:** Thank you so much for your presentation.

Earlier in your presentation, you made a reference to AI, artificial intelligence. Would you speak to how closely AI is connected with cybersecurity, autonomous vehicles and so on?

**Mr. Kerschbaum:** This is a very good question. I particularly like the question because it is a research question. We don't really know. What I can tell from what I understand about the problem is that there will be new threats due to machine learning, which we don't understand yet. We don't understand really what threats there could be. We get more of a glimpse as we go along. Of course there are many benefits to machine

**M. Kerschbaum :** Absolument.

**Le sénateur Wetston :** Avez-vous des suggestions à nous faire quant à la manière de procéder?

**M. Kerschbaum :** Cela déborde un peu de mon champ de compétence, mais je peux vous parler de mon expérience personnelle. Quand j'étais au secondaire, en Allemagne, il n'y avait pas de cours d'informatique. Maintenant, les élèves en dernière année du secondaire ont ce choix. C'est un grand pas en avant. Je crois aussi que savoir comment se servir de ce type de technologies est un élément clé de l'équation, de même qu'être au courant des principes de protection des données et de la vie privée, entre autres choses.

À la base, un ordinateur est un instrument mathématique, et plus on maîtrise les mathématiques, mieux on comprend l'informatique.

**Le sénateur Wetston :** Pour le secteur corporatif, notamment les grandes entreprises publiques — et pas seulement celles liées aux services financiers —, la cybersécurité est un des plus grands enjeux qui soient, aux côtés de la protection de la propriété intellectuelle, des données ou des services financiers, ou encore des changements climatiques, qui arrivent assez loin sur la liste. C'est ce qui ressort invariablement des rencontres des grands forums comme le Forum économique mondial, où les PDG de multinationales publiques présentent leur vision globale des affaires ou d'autres secteurs. Si c'est le cas, pensez-vous que nous ne prenons pas ce risque suffisamment au sérieux pour investir dans la sécurité ou les programmes d'éducation connexes? Et je fais référence autant au gouvernement qu'aux entreprises. Êtes-vous de cet avis?

**M. Kerschbaum :** En effet. C'est intéressant que vous ayez mentionné les changements climatiques, causés par la pollution, au nombre des grandes menaces. Bien sûr, sans réglementation, les entreprises ne feraient pas grand-chose pour prévenir la pollution. Il y a peut-être un parallèle à faire avec la cybersécurité.

**Le président :** Très intéressant.

**La sénatrice Unger :** Merci beaucoup pour votre témoignage.

Dans votre déclaration préliminaire, vous avez fait référence à l'intelligence artificielle. Pouvez-vous nous dire à quel point sont reliés l'intelligence artificielle et la cybersécurité, les véhicules autonomes et ces choses-là?

**M. Kerschbaum :** C'est une très bonne question. J'aime particulièrement cela, parce que cela renvoie à la recherche. Nous ne le savons pas vraiment. Ce que je peux vous dire, c'est qu'il y aura de nouvelles menaces issues de l'apprentissage machine, que nous ne comprenons pas encore. Nous ne savons pas comment ces nouvelles menaces pourraient se présenter. Les choses s'éclaircissent peu à peu, à mesure que la technologie se

learning that we want to preserve, but, at the same time, we want to prevent the threats. In some areas, we might not even have the right tools yet to do this properly. This is one aspect. The other aspect, of course, is that machine learning can also change the landscape of cybersecurity because, if I'm able to, for example, find attacks and replace the attacker using machine learning, then I also need to implement similar measures at the defence level. I'm trying, for example, to undertake some research projects where we can try to identify some of the vulnerabilities using machine learning. So there are a number of levels of interactions between the two topics. All of the levels I just mentioned are not fully understood yet.

développe. L'apprentissage machine offre de nombreux avantages, et nous voulons les préserver, mais nous voulons aussi prévenir les menaces. Dans certains cas, nous n'avons peut-être même pas les bons outils pour faire les choses correctement. C'est un côté de la médaille. De l'autre, l'apprentissage machine pourrait bien changer le paysage de la cybersécurité. Par exemple, si on trouve le moyen de remplacer les pirates par l'apprentissage machine pour mener des attaques, il faudra aussi développer des mesures semblables pour assurer la cyberdéfense. Je veux entre autres lancer des projets de recherche qui emploieront l'apprentissage machine afin de déceler des failles. Il y a donc effectivement des liens à faire entre les deux. Mais nous ne sommes pas encore en mesure de comprendre tout cela parfaitement.

**Senator Unger:** Thank you.

Would you just speak about encryption. Most banks have little signs that they are encrypted. What is the relationship between encryption and more along the lines of passwords, that kind of thing?

**La sénatrice Unger :** Merci.

Pouvez-vous nous parler du chiffrement? La plupart des banques ont une icône indiquant une communication chiffrée. Quel parallèle peut-on faire entre le chiffrement et les autres mesures de sécurité, comme les mots de passe?

**Mr. Kerschbaum:** The currently deployed encryption is excellent at protecting your data while it's being transmitted over the Internet or while it is stored on a disk. However, in between, there always is a gap. So the data is being encrypted on your side, sent to the bank, decrypted, processed, encrypted again and stored on disk. In between, that's where the vulnerabilities currently sit.

**M. Kerschbaum :** Le cryptage actuellement déployé excelle à protéger les données pendant leur transmission sur Internet ou leur stockage sur disque. Mais, entre les deux, une brèche subsiste, un talon d'Achille, entre le cryptage, l'envoi à la banque, le décryptage, le traitement et le cryptage de nouveau, puis le stockage sur disque.

Encryption is very strong.

Le cryptage est très fort.

One of my research goals for the last 11 years is trying to close this gap between those two things. It's still very expensive but theoretically doable. If you would go to something like defence in depth, and we can get encryption somewhat more cost effective in this intermediate step, then we might have a second layer that will help us protect against attacks where somebody breaks in.

L'un de mes objectifs de recherche, depuis 11 ans, est de fermer cette brèche. Cela reste très coûteux, mais, en théorie, c'est faisable. Si vous préfériez une défense en profondeur, nous pourrions opter pour un cryptage d'un meilleur rapport efficacité/coûts, dans cet intervalle, puis recouvrir le tout d'une deuxième couche qui le protégerait contre les attaques qui suivent une intrusion.

Right now, we need different measures. Particularly, we need to protect this space where encryption is not present. The former director of the Sirius Institute at Purdue once said, "Encrypting data over the Internet is like sending money from one bum on a park bench to another bum on a park bench." There is some truth to this; however, we also need to understand if we wouldn't have encryption, people probably would have attacked the armoured car in between, which is the encryption that protected us from all of this.

Actuellement, des mesures différentes s'imposent. Nous avons particulièrement besoin de protéger cet intervalle sans cryptage. L'ex-directeur de l'institut Sirius, à Purdue, a dit que crypter des données sur Internet, c'est comme envoyer de l'argent d'un clochard sur un banc de parc à un autre clochard sur un autre banc de parc. Il y a un fond de vérité là-dedans; mais il faut aussi comprendre que, faute de cryptage, le camion blindé qui circule entre les deux se serait peut-être fait attaquer. Le cryptage nous a protégés de cette éventualité.

Encryption is effective in mitigating this, but there is always residual risk. That residual risk is currently in this intermediate step where data is not easily encryptable at the moment. We need access to these accounts, like passwords and those things.

Le cryptage réduit efficacement ce risque, mais il en subsiste toujours un résidu. Ce risque résiduel se situe actuellement à cette étape intermédiaire où les données sont encore difficilement cryptables. Nous avons besoin d'accéder à ces comptes, par des mots de passe et ce genre de trucs.

There are efforts under way to bring more secure encryption, to replace passwords, for example. There is an initiative called the FIDO Alliance, where you would have a chip to plug into your computer that would replace all of your passwords in a very interesting way. I hope these things find more widespread use. They are implemented in some of the large software vendors' products, like Google and Microsoft, but I don't think any of you have come across this. I have one at home.

Again, we need to raise awareness that people actually use these types of tools and carry around this hardware token to replace passwords with cryptography.

**The Chair:** Professor, you are an excellent witness. You have been helpful to us. We are getting to the end of our study, so our questions are becoming very specific in terms of where we think we might want to go, and you have been very helpful. May I also say that, in my view, Waterloo is very lucky to have you, and I think Canada is lucky to have your expertise in this field. Thank you very much for your contribution today.

**Mr. Kerschbaum:** Thank you.

**The Chair:** Before introducing our next panel of witnesses — and we have an outstanding panel — I think it's useful if we spin around the table so you know the senators you will be interacting with after your presentations.

**Senator Tkachuk:** I'm Senator Tkachuk from Saskatchewan.

**Senator Stewart Olsen:** Carolyn Stewart Olsen, New Brunswick.

**Senator Wetston:** Howard Wetston, Ontario.

**Senator Marwah:** Sabi Marwah, Ontario.

**Senator Black:** Doug Black, Alberta.

[*Translation*]

**Senator Ringuette:** Pierrette Ringuette from New Brunswick.

[*English*]

**Senator Wallin:** Pamela Wallin, Saskatchewan.

**Senator Unger:** Betty Unger, Alberta.

[*Translation*]

**Senator Dagenais:** Jean-Guy Dagenais from Quebec.

[*English*]

**The Chair:** I have the pleasure of introducing to our committee members and those following these proceedings on the web, Colleen Merchant, Director General, National Cyber

On s'efforce actuellement de sécuriser davantage le cryptage, de remplacer les mots de passe, par exemple. Une initiative, l'alliance FIDO permet de brancher une puce dans l'ordinateur pour remplacer tous ses mots de passe de façon très intéressante. J'espère que ces nouveautés se généraliseront. Elles sont mises en œuvre dans certains produits de gros distributeurs de logiciels comme Google et Microsoft, mais je ne crois pas qu'un de vous en ait vu. J'en ai une chez moi.

Encore une fois, nous devons mieux nous rendre compte de l'utilisation de ces moyens qu'on emporte avec soi pour remplacer les mots de passe par la cryptographie.

**Le président :** Vous faites un excellent témoin. Vous nous avez été très utile. Nous arrivons à la fin de notre étude. Nos questions deviennent très pointues sur notre éventuel objectif, et vous nous avez beaucoup éclairés. Puis-je aussi ajouter que Waterloo est très chanceuse de vous avoir et je pense que le Canada est fortuné de pouvoir profiter de vos compétences dans ce domaine. Merci beaucoup de votre contribution.

**M. Kerschbaum :** Merci.

**Le président :** Avant de présenter notre prochain groupe de témoins, un groupe exceptionnel, je pense qu'il est utile de faire une sorte de tour de table pour présenter les sénateurs qui vous questionneront après vos exposés.

**Le sénateur Tkachuk :** Je suis le sénateur Tkachuk, de la Saskatchewan.

**La sénatrice Stewart Olsen :** Carolyn Stewart Olsen, du Nouveau-Brunswick.

**Le sénateur Wetston :** Howard Wetston, de l'Ontario.

**Le sénateur Marwah :** Sabi Marwah, de l'Ontario.

**Le sénateur Black :** Doug Black, de l'Alberta.

[*Français*]

**La sénatrice Ringuette :** Pierrette Ringuette, du Nouveau-Brunswick.

[*Traduction*]

**La sénatrice Wallin :** Pamela Wallin, de la Saskatchewan.

**La sénatrice Unger :** Betty Unger, de l'Alberta.

[*Français*]

**Le sénateur Dagenais :** Jean-Guy Dagenais, du Québec.

[*Traduction*]

**Le président :** J'ai le plaisir de présenter, aux membres de notre comité et à notre auditoire sur le Web, Mme Colleen Merchant, directrice générale de la cybersécurité nationale à

Security Directorate, at Public Safety Canada; Chief Superintendent Jeff Adam, Acting Assistant Commissioner, Technical Operations, Royal Canadian Mounted Police; and André Boucher, Associate Deputy Chief, IT Security, Communications Security Establishment.

I'm very delighted to have this panel here. You are the last panel we are going to be hearing from on this study, so we have a lot of questions for you, and we hope you have the answers.

We will start with statements, beginning with Ms. Merchant.

**Colleen Merchant, Director General, National Cyber Security Directorate, Public Safety Canada:** Thank you for inviting Public Safety Canada to speak to you on cybersecurity as it pertains to the recent Budget 2018 announcement.

As you know, Canadians are living in a digital age, and there is no aspect of our lives that has not been affected by digital technology and the Internet. The rate of technological change is continuing unabated.

[*Translation*]

Digital technology presents tremendous benefits and potential for Canada's economic prosperity and social development, but like any technology, it has its share of risks and dangers. Cybersecurity is the enabler that allows us to leverage the benefits of the digital age to the fullest while managing its risks.

[*English*]

In recognition of the new digital age, Budget 2018 proposed significant investments of $507.7 million over five years and $108.8 million per year ongoing thereafter to fund a new national cybersecurity strategy.

Today, I would like to talk about how cybersecurity has evolved within Canada, and highlight what we heard through the Cyber Security Review and how it influenced the new strategy and vision for cybersecurity going forward.

Canada's first cybersecurity strategy was published in 2010 as the government's plan for defending against cyberthreats. It was built on three pillars: securing Government of Canada systems; partnering to secure vital systems outside the federal government, and helping Canadians to be secure online.

The 2010 strategy represented the Government of Canada's view of cybersecurity as a defence against multiple cyberthreats. Cybersecurity has evolved, and like many of our allies, it has become a priority for the Government of Canada. The lens

Sécurité publique Canada, le surintendant principal Jeff Adam, qui est commissaire adjoint par intérim aux opérations techniques de la Gendarmerie royale du Canada, et M. André Boucher, qui est chef adjoint associé à la sécurité des TI au Centre de la sécurité des télécommunications.

Je suis ravi de vous accueillir. Vous êtes le dernier groupe de témoins pour cette étude. Nous avons donc beaucoup de questions pour vous et nous espérons que vous avez les réponses.

Nous commençons par les exposés, plus précisément celui de Mme Merchant.

**Colleen Merchant, directrice générale, Direction de la cybersécurité nationale, Sécurité publique Canada :** Merci d'avoir invité Sécurité publique Canada à venir vous parler de cybersécurité, relativement à l'annonce récente du budget de 2018.

Comme vous le savez, les Canadiens vivent dans une ère numérique, et aucun aspect de nos vies n'a échappé aux technologies numériques et à Internet. Le rythme des changements technologiques ne ralentit pas.

[*Français*]

La technologie numérique offre d'énormes avantages et possibilités pour la prospérité économique et le développement social du Canada. Cependant, comme toute technologie, elle présente son lot de risques et de danger. La cybersécurité est ce qui nous permet de tirer pleinement parti des avantages de l'ère numérique et d'en atténuer les risques.

[*Traduction*]

Reconnaissant l'avènement de cette ère numérique, le budget de 2018 a proposé un financement significatif à hauteur de 507,7 millions de dollars en cinq ans et de 108,8 millions par année, ensuite, d'une nouvelle Stratégie nationale de cybersécurité.

Aujourd'hui, je voudrais vous parler de l'évolution de la cybersécurité au Canada, mettre en relief ce que l'examen de la cybersécurité nous a appris et montrer son influence sur la nouvelle stratégie et la vision à venir de la cybersécurité.

Le Canada a publié sa première Stratégie nationale de cybersécurité en 2010. Elle était alors conçue comme le plan de défense du gouvernement contre les cybermenaces. Ses trois piliers étaient la sécurisation des systèmes du gouvernement du Canada; la formation de partenariats pour sécuriser les systèmes vitaux à l'extérieur de la fonction publique fédérale; l'aide aux Canadiens pour qu'ils se protègent en ligne.

La stratégie de 2010 représentait la perception qu'avait le gouvernement du Canada de la cybersécurité comme moyen de défense contre de multiples cybermenaces. La cybersécurité a évolué et, comme chez beaucoup de nos alliés, elle est devenue

through which we now look at cybersecurity is one through which we acknowledge the extent to which digital technologies have become essential to our way of life and how cybersecurity is an essential element of Canadian innovation and prosperity.

Our increasingly interconnected society is one in which all Canadians play an active role in shaping and sustaining our nation's cyber resilience. To that end, it's critical that governments, the private sector and academia work together to secure our digital infrastructure, create new opportunities, drive investment and foster leading-edge research and development.

You will likely recall in 2015 the Minister of Public Safety was mandated to lead a review of existing measures to protect Canadians and critical infrastructure from cyberthreats. The goal of the cyber review was to renew Canada's approach to cybersecurity.

[*Translation*]

An internal review included a review of federal cybersecurity governance, a review of the protections to Government of Canada systems, and the above-noted evaluation of Canada's cybersecurity strategy from 2010 to 2015.

[*English*]

Public consultations were conducted throughout 2016. Input was received from all provinces, two territories and internationally. Participants included government officials, the cybersecurity industry, private sector leaders and associations, critical infrastructure owners and operators, law enforcement, academia and engaged Canadians.

Three themes emerged in the review. First, participants expressed concern about the rising threat of cybercrime. There is support for law enforcement to address cybercrime while also protecting privacy in cyberspace.

Second, there is a need for improved cybersecurity skills and knowledge in Canada. Cyber skills shortages in the workforce make it challenging for organizations to improve cybersecurity. Knowledge is needed across all demographics in private and public sectors.

Third, there were calls for federal leadership on cybersecurity in several capacities. This includes clarifying cybersecurity roles, responsibilities and accountability within the federal government, as well as establishing a clear focal point for working with external partners. Stakeholders want the federal

une priorité du gouvernement. Le prisme au travers duquel nous la percevons maintenant nous révèle l'indispensabilité acquise par les technologies numériques pour notre mode de vie et le caractère essentiel de la cybersécurité pour l'innovation et la prospérité au Canada.

Dans notre société de plus en plus interconnectée, tous les Canadiens contribuent activement à l'établissement et au maintien de la cyberrésilience de notre pays, ce qui rend indispensable la collaboration des gouvernements avec le secteur privé et les universités pour sécuriser nos infrastructures numériques, créer des occasions, stimuler l'investissement et favoriser la recherche-développement de pointe.

Vous vous rappellerez peut-être que, en 2015, le ministre de la Sécurité publique a été chargé de diriger un examen des mesures alors en vigueur pour protéger les Canadiens et les infrastructures essentielles contre les cybermenaces. L'objectif de l'examen était de renouveler la démarche cybersécuritaire du Canada.

[*Français*]

L'examen interne comprenait un examen de la gouvernance fédérale en matière de cybersécurité, un examen de protection des systèmes de gouvernement du Canada et l'évaluation susmentionnée de la Stratégie nationale de cybersécurité du Canada de 2010 à 2015.

[*Traduction*]

Des consultations publiques ont eu lieu pendant tout 2016. Y ont participé toutes les provinces, deux territoires et des intervenants de l'étranger. Les participants étaient notamment des fonctionnaires, l'industrie de la cybersécurité, des dirigeants et associations du secteur privé, des propriétaires et exploitants d'infrastructures essentielles, des représentants d'organisations policières, des universités et des Canadiens intéressés.

Elles ont ainsi dégagé trois grands thèmes. D'abord, les participants se disaient inquiets devant la menace croissante de la cybercriminalité. On appuyait l'action de la police pour combattre la cybercriminalité tout en protégeant aussi la vie privée dans le cyberespace.

Ensuite, il fallait améliorer les compétences et les connaissances au Canada en matière de cybersécurité. Les lacunes dans les cybercompétences, chez les actifs, compliquaient la tâche d'améliorer la cybersécurité dans les organisations. Il fallait augmenter les connaissances dans toutes les tranches d'âge des effectifs des secteurs privé et public.

Enfin, on a réclamé l'initiative fédérale à plusieurs titres en matière de cybersécurité, notamment la clarification des rôles, des responsabilités et la responsabilisation à l'échelon fédéral, de même que la création d'un pôle bien visible de collaboration avec les partenaires de l'extérieur. Les joueurs veulent que l'État

government to take a leading role domestically and internationally to foster collaboration among cybersecurity experts, drive investment in the cybersecurity industry, facilitate information sharing, and safeguard rights and freedoms in cyberspace. There were also calls for the federal government to articulate national cybersecurity standards for legislation.

The national cybersecurity strategy responds to the findings of the Cyber Review and introduces a new direction for cybersecurity. The strategy defines three goals to achieve security and prosperity in the digital age. The first is secure and resilient Canadian systems with enhanced capabilities and collaboration with partners; the Government of Canada will better protect Canadians from cybercrime, respond to evolving threats, and help defend critical government and private sector systems. The second is an innovative and adaptive cyber ecosystem. The Government of Canada will support advanced research, foster digital innovation and develop cyber skills and knowledge to position Canada as a global leader in cybersecurity. Third, effective leadership, governance and collaboration. The federal government, in collaboration with provinces, territories and the private sector, will take a leadership role to advance cybersecurity in Canada and will, in coordination with allies, work to shape the international cybersecurity environment in Canada's favour.

[*Translation*]

This new approach reflects the dynamic evolution of digital technologies and the extent to which they have become essential to our way of life. It also recognizes that there is enormous potential for Canadian digital innovation and expertise in cybersecurity.

[*English*]

The strategy, which is meant to be a guiding framework, includes numerous initial initiatives. Key among them is a consolidated centre of cybersecurity operations, the Canadian centre for cybersecurity, to be led by the Communications Security Establishment and a national cybercrime coordination unit within the RCMP as a national police service.

I'll let the respective leads for each of these initiatives speak to them.

From a departmental perspective, Public Safety received roughly $25 million over five years in support of the new strategy. While the allocation of those funds has not yet been fully determined, Public Safety Canada will retain its

fédéral se charge d'un rôle de premier plan à l'échelle nationale et sur la scène internationale, pour favoriser la collaboration entre les spécialistes de la cybersécurité, diriger les investissements vers l'industrie de la cybersécurité, faciliter la mise en commun de l'information et sauvegarder les droits et libertés dans le cyberespace. On demande aussi à l'État fédéral d'énoncer des normes nationales de cybersécurité pour l'édiction de lois.

La Stratégie nationale de cybersécurité fait suite aux constatations de l'examen de la cybersécurité et lui imprime une orientation nouvelle. Elle précise trois objectifs pour atteindre la sécurité et la prospérité dans l'ère numérique. Le premier est de doter les systèmes canadiens sécurisés et résilients de capacités augmentées, grâce à une collaboration plus grande avec les partenaires; le gouvernement du Canada protégera mieux les Canadiens contre la cybercriminalité, il réagira à l'évolution des menaces et aidera à la défense des systèmes essentiels à l'État et au secteur privé. Le deuxième est un cyberécosystème innovant et adaptable. Le gouvernement du Canada appuiera la recherche de pointe, il encouragera l'innovation numérique et développera les cybercompétences et les cyberconnaissances pour positionner le Canada parmi les chefs de file mondiaux de la cybersécurité. Troisième objectif : il faut une direction, une gouvernance et une collaboration efficaces. L'État fédéral, en collaboration avec les provinces, les territoires et le secteur privé, jouera un rôle de premier plan pour promouvoir la cybersécurité au Canada et, en coordination avec ses alliés, il travaillera à modifier l'environnement international de la cybersécurité en faveur du Canada.

[*Français*]

Cette nouvelle approche correspond à l'évolution dynamique des technologies numériques et montre combien elles sont devenues essentielles à notre mode de vie. Elle reconnaît aussi l'énorme potentiel pour ce qui est de l'innovation et de l'expertise numérique canadienne dans le domaine de la cybersécurité.

[*Traduction*]

La stratégie, qui se veut un ensemble de mesures d'orientation, englobe de nombreuses initiatives initiales. Parmi elles, un centre fusionné d'opérations de cybersécurité, le Centre canadien pour la cybersécurité, qui sera dirigé par le Centre de la sécurité des télécommunications, et une Unité nationale de coordination de la lutte contre la cybercriminalité, à la GRC, comme service national de police, occuperont une place à part.

Je laisserai aux animateurs respectifs de chacune de ces initiatives le soin d'en parler.

Le ministère de la Sécurité publique a reçu en gros 25 millions de dollars sur cinq ans pour la nouvelle stratégie. Même si l'affectation de ces fonds n'est pas encore tout à fait arrêtée, le ministère conservera ses responsabilités dans la direction de la

responsibility for leading national coordination and strategic policy-making on cybersecurity matters. In particular, Public Safety will continue to work with its provincial and territorial partners as well as partners in the federal government, private sector and academia to meet the goals of the new strategy. One of the ways this work will continue to be supported is through a grant and contributions program to encourage research and activities to advance the goals of the strategy.

[*Translation*]

Public Safety Canada is also seeking funding to deliver a comprehensive risk management approach that will enable critical infrastructure owners and operators to better secure their systems and information.

[*English*]

This approach would involve building upon successful programs that work directly with owners and operators to help build resilience. Owners and operators would have more access to technical training, exercises and network vulnerability assessments, providing the knowledge and skills they need to take action to secure their cyber systems.

Finally, Public Safety Canada will continue to oversee the implementation of the national cybersecurity strategy and measure its progress against the commitments made within. As such, the department will work closely with the new Canadian centre for cybersecurity as well as the national cybercrime coordination unit to ensure our efforts are coordinated and comprehensive as we deliver on this first phase of the strategy.

[*Translation*]

In closing, I would emphasize that cyberthreats are constantly evolving, and Canada and Canadians need to work to stay ahead of those threats, so that we can continue to benefit from digital technology.

[*English*]

Public Safety enjoys good relationships and frequent interactions with financial institutions across Canada, and we look forward to continuing that collaboration.

Thank you again for the opportunity to speak with you today. I look forward to any questions that you might have.

**Chief Superintendent Jeff Adam, Acting Assistant Commissioner, Technical Operations, Royal Canadian Mounted Police:** Good afternoon Mr. Chair and members of the committee. Thank you for inviting the Royal Canadian

coordination nationale et la prise de décisions stratégiques en matière de cybersécurité. Il continuera notamment de collaborer avec ses homologues des provinces et des territoires ainsi que ses partenaires de l'administration fédérale, le secteur privé et les universités pour atteindre les objectifs de la nouvelle stratégie. On continuera notamment d'appuyer ce travail au moyen d'un programme de subventions et de contributions pour encourager la recherche et les activités permettant d'atteindre plus rapidement ces objectifs.

[*Français*]

Sécurité publique Canada cherche aussi des fonds pour mettre en application une méthode de gestion des risques globale qui permettra aux propriétaires et exploitants d'infrastructures essentielles de mieux protéger leurs systèmes et leurs données.

[*Traduction*]

À cette fin, on misera sur des programmes couronnés de réussite de collaboration directe avec les propriétaires et exploitants de réseaux pour les aider à en augmenter la résilience. Ils auraient davantage accès à une formation technique, à des exercices et à des évaluations de la vulnérabilité de leur réseau, qui leur procureraient les connaissances et les compétences nécessaires pour qu'ils sécurisent leurs cybersystèmes.

Enfin, Sécurité publique Canada continuera de surveiller la mise en œuvre de la Stratégie nationale de cybersécurité et en mesurera les progrès par rapport aux engagements internes. À ce titre, le ministère collaborera étroitement avec le nouveau Centre canadien pour la cybersécurité ainsi qu'avec l'Unité nationale de coordination de la lutte contre la cybercriminalité pour assurer la coordination et l'exhaustivité de nos efforts dans cette première étape de la stratégie.

[*Français*]

En conclusion, je tiens à mettre l'accent sur le fait que les cybermenaces sont en constante évolution et que le Canada et les Canadiens doivent faire en sorte d'avoir une longueur d'avance en la matière pour que nous puissions continuer de tirer parti de la technologie numérique.

[*Traduction*]

Sécurité publique Canada a noué des relations excellentes et assidues avec les établissements financiers de tout le Canada et il compte poursuivre cette collaboration.

Merci encore de votre invitation à venir témoigner. Je suis prête à répondre à vos questions.

**Surintendant principal Jeff Adam, commissaire adjoint par intérim, Opérations techniques, Gendarmerie royale du Canada :** Bonjour, monsieur le président, mesdames et messieurs les membres du comité. Merci d'avoir invité la GRC à

Mounted Police to speak about cybercrime in Canada and recent initiatives announced in the federal government's 2018 Budget.

[*Translation*]

To begin, I would like to take some time to provide the broader context within which the RCMP's activities relating to cybercrime are taking place.

[*English*]

Cybercrime is a significant public safety and law enforcement issue in Canada and a complex problem that no single organization can resolve. In spite of issues with public underreporting, cybercrime in Canada appears to be increasing. In 2016, nearly 24,000 cybercrimes were reported to Canadian police services, a 58 per cent increase compared to 2014.

Globally, the annual economic costs of cybercrime have been estimated to be in the hundreds of billions of dollars. When it comes to Canada's financial and commercial sectors, the volume and severity of cybercrime affecting Canadians and businesses has also been increasing significantly.

Cybercrime includes new crimes such as hacking, network intrusions and data theft which are technology-as-target crimes. It also includes more traditional crimes that take on a new scope and magnitude in cyberspace such as online fraud scams, money laundering, child sexual exploitation which we call technology as an instrument crime.

As Canada's national police force, the RCMP has a broad mandate to investigate criminals in the cyber realm resulting in their apprehension or otherwise disrupting their cybercrime activity. Law enforcement activities range from identifying and prioritizing cybercrime threats based on criminal intelligence to investigating and disrupting cybercrime activities to handling digital evidence in support of cybercrime investigations.

For law enforcement, addressing cybercrime requires broad-based domestic and international police cooperation, integrating new technical skills and tools with traditional enforcement measures and engagement with public and private sector organizations, including those within the financial sector. The RCMP cybercrime strategy published in 2015 reflects this role of cyber in several law enforcement areas including national coordination and deconfliction, intelligence collection and analysis, targeted enforcement and investigative action and specialized skills, tools and training.

venir parler de la cybercriminalité au Canada et des initiatives récentes annoncées dans le budget fédéral de 2018.

[*Français*]

Pour commencer, j'aimerais prendre le temps de présenter le contexte dans lequel se déroulent les activités en matière de cybercriminalité de la GRC.

[*Traduction*]

La cybercriminalité est un important problème de sécurité publique et d'application de la loi au Canada et un problème complexe qu'une organisation ne peut pas régler toute seule. Même si tous les cas ne sont pas signalés par le public, elle semble prendre de l'ampleur au Canada. En 2016, près de 24 000 cybercrimes ont été signalés à la police, soit une augmentation de 58 p. 100 par rapport à 2014.

À l'échelle mondiale, on a estimé les coûts économiques annuels de la cybercriminalité à des centaines de milliards de dollars. En ce qui concerne le secteur financier et le secteur commercial au Canada, le volume et la gravité de la cybercriminalité dont sont victimes les Canadiens et les entreprises ont également augmenté considérablement.

La cybercriminalité comprend de nouveaux crimes tels que le piratage informatique, les intrusions dans les réseaux et le vol de données, qui sont des crimes visant la technologie. Elle englobe également les crimes plus traditionnels, qui prennent une envergure et une importance nouvelles dans le cyberespace, tel que les escroqueries en ligne, le blanchiment d'argent et l'exploitation sexuelle des enfants, qui sont des crimes commis au moyen de la technologie.

En tant que service national de police du Canada, la GRC a le vaste mandat d'enquêter sur les criminels dans l'espace cybernétique afin de les arrêter ou de perturber leurs activités. Pour appliquer la loi, elle s'emploie à déterminer les menaces de cybercrime et à en établir l'ordre de priorité jusqu'à fournir des preuves numériques à l'appui des enquêtes, en passant par le renseignement criminel, les enquêtes sur les activités criminelles dans le cyberespace et la perturbation de ces activités.

Pour les organismes d'application de la loi, la lutte contre la cybercriminalité exige une vaste coopération entre les polices nationales et étrangères, qui intègre de nouvelles compétences techniques et de nouveaux outils aux mesures d'application traditionnelles de la loi, et qui exige un engagement avec les organisations du secteur public et privé, y compris celles du secteur financier. La stratégie de lutte contre la cybercriminalité de la GRC, publiée en 2015, fait état du rôle cybernétique dans plusieurs secteurs d'application de la loi, y compris la coordination et l'harmonisation à l'échelle nationale, la collecte et l'analyse de renseignements, des mesures de répression et d'enquête adaptées, ainsi que des compétences, de la formation et des outils spécialisés.

Despite progress to date, law enforcement has faced significant barriers to combatting cybercrime in Canada. The Canadian policing model is predicated on the assumption that the offender, the victim and the justice system are largely co-located jurisdictionally. However, as we know, most cybercrimes are multi-jurisdictional if not multinational, impacting victims across traditional jurisdictions, leading to uncoordinated law enforcement efforts.

Traditional investigative tools are not designed for the volatility of data nor the fluidity of information pathways in today's digital environment.

Law enforcement requires a means to gather information and intelligence regardless of jurisdiction, and a mechanism to coordinate investigative efforts. It is not efficient for multiple police services to be allocating scarce investigative resources on the same criminal activity in an isolated fashion. In addition, cybercrime is believed to be underreported and there are varied reporting mechanisms in Canada, which is confusing for the public. This underreporting prevents law enforcement from connecting the dots and responding to cybercrime on a larger coordinated and more targeted scale. Gaps also exist with respect to the RCMP's capacity to investigate cybercrime limiting its ability to undertake necessary enforcement action.

To address these challenges and bolster Canada's ability to fight cybercrime the government recently announced $116 million over five years and $23.2 million per year ongoing devoted to the creation of the RCMP national cyber crime coordination unit.

The unit will be a national police service, stewarded by the RCMP, supporting and working with law enforcement across Canada. It will act as a coordination hub for cybercrime investigations in Canada and will work with international partners on cybercrime. It will provide digital investigative advice and guidance to Canadian law enforcement, undertake intelligence and statistical analysis and forge and maintain strategic partnerships with key stakeholders, including the private sector. The recently announced Canadian Centre for Cyber Security will be a vital partner for the unit. The unit will also establish a national public reporting mechanism for Canadian citizens and businesses to report cybercrime incidents to law enforcement, which will address underreporting of cybercrime and greatly improve law enforcement's understanding of the nature and scope of cybercrime in Canada.

Malgré les progrès réalisés à ce jour, les organismes d'application de la loi doivent vaincre d'importants obstacles dans leur lutte contre la cybercriminalité au Canada. Le modèle de service de police canadien est basé sur l'hypothèse selon laquelle le délinquant, la victime et le système de justice relèvent pour la plupart de la même autorité judiciaire. Toutefois, comme nous le savons, la plupart des cybercrimes se commettent dans plusieurs juridictions sinon dans plusieurs pays, et ils ont une incidence sur des victimes dans l'ensemble des administrations traditionnelles, ce qui désorganise l'application de la loi.

Les outils traditionnels d'enquête sont mal adaptés à la volatilité des données et à la fluidité des voies d'information dans l'environnement numérique d'aujourd'hui.

Les organismes d'application de la loi ont besoin d'un moyen d'obtenir de l'information et du renseignement, peu importe l'administration, et d'un mécanisme visant à coordonner les efforts d'enquête. Il n'est pas efficient pour les divers services de police d'affecter leurs maigres ressources d'enquête à la même activité criminelle, chacun pour soi. De plus, on croit que tous les cas de cybercriminalité ne sont pas déclarés, et les divers mécanismes de signalement employés au Canada sèment la confusion chez le public. La déclaration partielle des crimes déforme la réalité et empêche une lutte à plus grande échelle, mieux coordonnée et mieux ciblée.

Pour relever ces défis et renforcer la capacité du Canada de lutter contre la cybercriminalité, le gouvernement a récemment annoncé 116 millions de dollars sur cinq ans et 23,2 millions par année, par la suite, afin de mettre sur pied l'Unité nationale de coordination de la lutte contre la cybercriminalité de la GRC.

L'unité sera un service de police national, supervisé par la GRC, appuyant les organismes d'application de la loi dans l'ensemble du Canada et collaborant avec eux. Elle servira de centre de coordination des enquêtes sur les cybercrimes au Canada et unira ses efforts à ceux des partenaires étrangers pour lutter contre la cybercriminalité. Elle fournira conseils et avis pour les enquêtes sur la cybercriminalité aux organismes canadiens d'application de la loi, entreprendra une analyse du renseignement et des statistiques et établira et maintiendra des partenariats stratégiques avec des intervenants principaux, y compris le secteur privé. Le Centre canadien pour la cybersécurité récemment annoncé sera un partenaire essentiel de l'unité. L'unité établira un mécanisme national de signalement public afin que les citoyens et les entreprises du Canada signalent les incidents de cybercriminalité aux organismes d'application de la loi, ce qui réglera le problème de leur sous-déclaration et améliorera grandement la compréhension des organismes d'application de la loi quant à la nature et à la portée de la cybercriminalité au Canada.

Through these new investments, the RCMP will play a critical role in advancing Canada's new National Cyber Security Strategy and will be better positioned to reduce the threat, impact and victimization of cybercrime in Canada.

Thank you for your time. I would be pleased to answer any questions.

**The Chair:** Thank you. We will now hear from André Boucher, Associate Deputy Chief, IT Security, Communications Security Establishment.

**André Boucher, Associate Deputy Chief, IT Security, Communications Security Establishment:** Good afternoon, Mr. Chair and members of the committee. I would like to start by thanking the committee for inviting me to speak alongside my colleagues from RCMP and Public Safety. It is a pleasure to appear before you to discuss cybersecurity in Canada. As Associate Deputy Chief for Information Technology Security, this is an issue near and dear to my heart. In the interest of time, and recognizing that CSE has already appeared before you as part of your study, I won't speak in any detail to CSE's mission or mandate. Instead, I will briefly elaborate on cybersecurity elements related to CSE that were announced as part of Budget 2018.

As Ms. Merchant described, Budget 2018 announced significant investments in Canada's cybersecurity, including the newly proposed Canadian centre for cybersecurity.

[*Translation*]

This new centre will form the centerpiece of the government's planned cybersecurity strategy to bolster the safety of Canadians and Canadian businesses online. One of the main concepts behind the centre is to concentrate the government's expertise and cybersecurity tools in one place.

The fact is that most of that expertise is already at CSE. CSE has been in the business of protecting Canada's most sensitive information for over 70 years. As Canada's centre of excellence for cyberoperations, CSE will house the Canadian Centre for Cyber Security, bringing together operational expertise from CSE and our colleagues at Public Safety Canada and Shared Services. By consolidating operational cyberexpertise from across the federal government under one roof, the new cybercentre will establish a single, unified Government of Canada source of unique expert advice, guidance, services and support on cybersecurity operational matters, providing Canadian citizens and businesses with a clear and trusted place to turn to for cybersecurity advice.

Grâce à ces nouveaux investissements, la GRC jouera un rôle essentiel dans l'avancement de la nouvelle Stratégie nationale de cybersécurité du Canada et elle sera mieux positionnée pour réduire la menace, l'impact et la victimisation liés à la cybercriminalité au Canada.

Merci de votre temps. Je serai heureux de répondre à toutes vos questions.

**Le président :** Merci. Nous allons maintenant entendre André Boucher, qui est chef adjoint associé, Sécurité des TI, pour le Centre de la sécurité des télécommunications.

**André Boucher, chef adjoint associé, Sécurité des TI, Centre de la sécurité des télécommunications :** Bonjour, monsieur le président et distingués membres du comité. J'aimerais d'abord remercier le comité de m'avoir invité à prononcer quelques mots en compagnie de mes collègues de la GRC et de Sécurité publique. C'est avec plaisir que je me présente devant vous pour discuter de la cybersécurité au Canada. En tant que chef adjoint associé à la Sécurité des technologies de l'information, il va sans dire qu'il s'agit d'un sujet qui me tient à cœur. Par souci de concision, et dans la mesure où le CST s'est déjà présenté devant vous dans le cadre de la présente étude, je ne parlerai pas de la mission et du mandat du CST. Je vous donnerai plutôt quelques détails concernant les éléments de cybersécurité associés au CST qui ont été annoncés lors du budget de 2018.

Comme l'a décrit Mme Merchant, le budget de 2018 fait mention d'importants investissements dans la cybersécurité du Canada, notamment le nouveau Centre canadien pour la cybersécurité.

[*Français*]

Le nouveau centre constituera la pièce maîtresse de la Stratégie nationale de cybersécurité que le gouvernement mettra en œuvre pour accroître la sécurité des Canadiens et des entreprises canadiennes en ligne. L'un des principaux concepts visés par la création du centre est de rassembler l'expertise et les outils du gouvernement en matière de cybersécurité sous un même toit.

Le fait est que la majorité de cette expertise existe aujourd'hui au CST. Le CST veille à la protection des renseignements les plus sensibles du Canada depuis plus de 70 ans. En tant que centre d'excellence du Canada en matière de cyberopérations, l'organisme hébergera le Centre canadien pour la cybersécurité, réunissant du même coup l'expertise opérationnelle du CST et celle de ses collègues de Sécurité publique Canada et de Services partagés. En regroupant sous un seul toit la cyberexpertise opérationnelle du gouvernement fédéral, le nouveau centre permettra au gouvernement du Canada de disposer d'une source unifiée de conseils, d'orientations, de services et de soutien spécialisés concernant les questions opérationnelles liées à la cybersécurité. Ainsi, les citoyens et les entreprises du Canada

For Canada, this will mean faster, better coordinated and more coherent government responses to cyberthreats. In addition, it will mean better information flow between the government and private sector partners. This cybercentre will also advance partnerships and dialogue with other jurisdictions, the business community, academia and international partners. Ultimately, it will mean stronger cyberprotection and defence for the government, the private sector and Canadians.

As set out in our earlier appearance, partnerships are key to our success. This is why the newly proposed Canadian Centre for Cyber Security is an exciting step forward for cybersecurity in Canada.

[*English*]

In closing, I would like to once again thank the committee for the opportunity to speak to you this afternoon and I look forward to your questions.

**The Chair:** Thank you all very much. We will move to questions.

**Senator Stewart Olsen:** Thank you all for being here. It's most informative. I've come late to this study so forgive me if I ask questions that you've been over.

In reviewing what you have said and the budget proposal, I'm curious about the new Canadian centre for cyber security. From what you're saying, Mr. Boucher, you're going to be front and centre in this new exercise. How is that going to work with your collaboration and cooperation with the RCMP and different areas? I'm not 100 per cent sure that I understand how you're going to be able to work with everyone and how much you are going to expand. This is not a lot of money for what I think you're being asked to do. Can you elaborate on how you see this unfolding?

**Mr. Boucher:** Thank you for your queston. I think the key message in the budget is led by CSE in regrouping elements of the federal entities of cybersecurity. This is a recognition that separate organizations are currently operating in cybersecurity but perhaps not as efficiently or effectively as they could. To your point about the resources, we are taking existing organizations, existing manpower, and bringing them together to create that coherence and do better with the existing resources. That might explain your puzzled question regarding resources.

pourront compter sur une source bien établie et fiable de conseils en matière de cybersécurité.

Pour le Canada, la mise en place du centre se traduira par des interventions du gouvernement plus rapides, mieux coordonnées, et plus cohérentes en cas de cybermenace, ainsi que par une meilleure communication des informations entre le gouvernement du Canada et ses partenaires du secteur privé. De plus, le centre fera avancer les partenariats et le dialogue avec d'autres administrations, avec le milieu des affaires, le milieu universitaire, et les partenaires internationaux. Enfin, le centre permettra d'accroître la cyberprotection et la défense du gouvernement, du secteur privé et des Canadiens.

Comme il a été mentionné précédemment, les partenariats sont essentiels à la réussite de la mission de notre organisme. C'est pourquoi la mise en place du nouveau Centre canadien pour la cybersécurité marque une étape déterminante pour la cybersécurité au Canada.

[*Traduction*]

En conclusion, je tiens à remercier encore une fois le comité de m'avoir donné l'occasion de m'adresser à vous cet après-midi et je serai heureux de répondre à vos questions.

**Le président :** Merci beaucoup à tous. Nous allons maintenant passer aux questions.

**La sénatrice Stewart Olsen :** Nous vous remercions de votre présence ici aujourd'hui. Vos témoignages nous sont très utiles. Je suis arrivée tard dans cette étude alors vous me pardonnerez si je soulève des questions que vous avez déjà abordées.

Après vous avoir entendu et avoir examiné la proposition de budget, je suis curieuse d'en apprendre plus sur le nouveau Centre canadien pour la cybersécurité. D'après ce que vous dites, monsieur Boucher, vous ferez un travail d'avant-plan à cet égard. Comment allez-vous collaborer avec la GRC et les divers secteurs? Je ne suis pas certaine de comprendre comment vous allez pouvoir travailler avec tout le monde et accroître vos activités. Ce n'est pas beaucoup d'argent pour ce qu'on vous demande de faire. Pouvez-vous nous expliquer comment tout cela se déroulera?

**M. Boucher :** Je vous remercie de votre question. Je crois que le message clé dans le budget, c'est que le CST sera responsable de regrouper les éléments des entités fédérales en matière de cybersécurité. On reconnaît que le travail des organisations distinctes en matière de cybersécurité n'est peut-être pas aussi efficace qu'il devrait l'être. Pour répondre à votre question au sujet des ressources, nous prenons les organisations existantes, les effectifs en place, et nous les regroupons afin d'uniformiser le travail et d'accroître l'efficacité des ressources existantes. Cela répond peut-être à votre questionnement au sujet des ressources.

A lot of good is being done in the federal government today. It has grown out of necessity in different departments. A time came when we realized that there was an entire duplication. There may have been some overlap and friction between these departments, and then the coherence started to disappear. For our clients, whether it be the federal government or partners in the private sector, it became confusing. What's absolutely central to the announcement is the fact we are now bringing these elements together all in one leadership. As to the how, we need to know the plan and build the centre.

It is reasonable to expect that the very first effort will be focused on bringing the elements fused together— CSE, Public Safety and Shared Services— and create harmony between us. Maybe the analogy is then to create a single door for the government.

When it comes to the cybercrime unit and other entities operating in cyber, they will continue to exist, but since we have the opportunity to build a centre together, we can build our activities at the same time and ensure that the synchronicity is there from the ground up.

This is an opportunity to reset and do better with resources that we have in place.

**Senator Stewart Olsen:** I do understand. My hesitation is there doesn't seem to be anyone in charge. I don't think that's a recipe for success, quite frankly. I think this is going to have to move fairly quickly. It has been announced, and we have to bring this all together fairly quickly. We have no one really designated as in charge, and everyone is going to think they're in charge. Could you please comment a bit on that?

**Mr. Boucher:** Absolutely. I would say that CSE certainly feels in charge of the portion apportioned to us.

**Senator Stewart Olsen:** A portion.

**Mr. Boucher:** Absolutely. And I think it's inevitable for the community to work together.

**An Hon. Senator:** What's your portion?

**Mr. Boucher:** The integration of the CSE activities in cybersecurity with the Public Safety CCIRC activities and the Government of Canada's security operations centres at Shared Services. That's a significant amount of resources which currently coexist.

We know we are responsible to bring this element together, and I think we are going to do a surprising amount of work just by creating this team approach.

**Senator Stewart Olsen:** Ms. Merchant, in your presentation, one of the key points was education and encouraging education to provide us with the expertise that we're going to need as we

On fait beaucoup de bon travail au gouvernement fédéral. C'est une question de nécessité pour les ministères. Nous avons constaté qu'il y avait un important chevauchement et des frictions entre les ministères, et qu'il y avait de moins en moins d'uniformité. Pour nos clients, qu'il s'agisse du gouvernement fédéral ou de nos partenaires du secteur privé, c'était déroutant. Ce qui est au cœur de cette annonce, c'est le regroupement de ces éléments sous une direction unique. Quant à la façon de faire, nous devons avoir un plan et construire le centre.

Il est raisonnable de s'attendre à ce que la toute première étape consiste à fusionner les éléments — le CST, Sécurité publique et Services partagés — et à créer une harmonie entre nous. On peut faire une analogie et dire qu'il y aura un guichet unique pour le gouvernement.

En ce qui a trait à l'unité de la cybercriminalité et aux autres entités qui travaillent dans le domaine cybernétique, elles existeront toujours, mais comme nous avons l'occasion de bâtir un centre ensemble, nous allons pouvoir établir nos activités ensemble et assurer un synchronisme dès le départ.

Nous avons l'occasion de repartir à neuf et de faire un meilleur travail avec les ressources en place.

**La sénatrice Stewart Olsen :** Je comprends. Ce qui me fait hésiter, c'est qu'il ne semble pas y avoir de responsable. Je ne crois pas que ce soit la recette du succès, bien franchement. Je crois qu'il faudra faire les choses assez rapidement. On a fait l'annonce et il faut regrouper tous ces éléments assez rapidement. On n'a pas désigné de responsable et tout le monde voudra décider. Pourriez-vous commenter cela?

**M. Boucher :** Tout à fait. Je dirais que le CST est responsable de la partie qui nous est attribuée.

**La sénatrice Stewart Olsen :** Une partie.

**M. Boucher :** Tout à fait. Et je crois qu'il faut que les membres de la communauté travaillent ensemble.

**Une voix :** De quelle partie êtes-vous responsable?

**M. Boucher :** De l'intégration des activités du CST en matière de cybersécurité à celles du CCRIC de Sécurité publique et des centres des opérations de la sûreté du gouvernement du Canada à Services partagés. C'est une quantité importante de ressources qui coexistent à l'heure actuelle.

Nous savons que nous sommes responsables de regrouper ces éléments et je crois que déjà, en créant une approche d'équipe, nous allons accomplir un travail très important.

**La sénatrice Stewart Olsen :** Madame Merchant, dans votre exposé, vous avez parlé de favoriser l'éducation afin d'obtenir l'expertise dont nous allons avoir besoin pour l'élaboration de

develop this grant, but I didn't hear anything in your presentation about how you will do that.

We have all kinds of centres of excellence in academics, et cetera, but those people, they're already the experts, and we don't have enough of them. What are you looking at, and how will you move forward to develop this?

**Ms. Merchant:** There are many things that we're already doing that we will be looking to enhance. For example, we work very closely with academic institutions as they build new and exciting programs around cybersecurity, and we have our grants and contributions program which many universities take advantage of. We've had Ryerson and a few others that have taken advantage of that funding to perform research, build into their academic baseline some of these skill sets that we're looking for.

In addition, education and skills development at a level lower than universities and so forth, that is the purview of the provinces and territories.

As I had mentioned, something that will be extremely important to us is to not just continue those relationships with the provinces and territories so that we're collectively moving in the same direction toward the same priorities in academics and skills development, but to enhance what we're already doing and through the grants and contributions program funnel some of this direction to the universities, to the lower levels of education.

I do want to point out in the cybersecurity review, we heard loud and clear that it would be very important for us to consider how we get those skills developing, even at the elementary level. So that is something we're very sensitive to.

**Senator Stewart Olsen:** Thank you.

**Senator Wallin:** Thank you for being here today. When you talked about the $500 million over five years on a national cybersecurity strategy, as I listened to you, what I heard is that you're constructing a framework, a bureaucracy, who talks to whom, when, how, and you're talking about the issue. Is there any portion of that money that actually goes to tools, equipment, monitoring, or is this just setting up a framework?

**Ms. Merchant:** In terms of the strategy itself, there are two different things. There is the strategy itself, which lays out the three goals we want to move to, and then there was the funding associated with the initiatives to deliver on the strategy.

**Senator Wallin:** Give me an example of one of those things.

**Ms. Merchant:** The initiatives? The cyber centre or the national cybercrime coordination unit.

cette subvention, mais je ne vous ai pas entendu dire comment vous y arriveriez.

Nous avons toutes sortes de centres d'excellence dans les études et tout cela, mais ces gens sont déjà les experts et nous n'en avons pas suffisamment. Comment allez-vous procéder pour aller de l'avant?

**Mme Merchant :** Nous en faisons déjà beaucoup et nous allons accroître nos activités. Par exemple, nous travaillons en étroite collaboration avec les établissements universitaires alors qu'ils créent de nouveaux programmes très intéressants dans le domaine de la cybersécurité; nous avons un programme de subventions et contributions, dont profitent de nombreuses universités. L'Université Ryerson et quelques autres ont profité de ce financement pour faire des travaux de recherche et intégrer les ensembles de compétences que nous préconisons.

De plus, l'éducation et le développement des compétences à un niveau inférieur relèvent des provinces et des territoires.

Comme je l'ai dit plus tôt, il sera très important pour nous non seulement de maintenir les relations avec les provinces et les territoires de manière à aller dans la même direction et à avoir les mêmes priorités en matière de formation et de perfectionnement des compétences, mais aussi de transmettre notre orientation aux universités et aux autres établissements d'études par l'entremise du programme de subventions et de contributions.

Je tiens à souligner que dans le cadre de l'examen de la cybersécurité, nous avons bien compris qu'il était important de déterminer comment développer les compétences, même au niveau élémentaire. Nous sommes donc très sensibles à cela.

**La sénatrice Stewart Olsen :** Merci.

**La sénatrice Wallin :** Nous vous remercions de votre présence ici aujourd'hui. Lorsque vous avez parlé de 500 millions de dollars sur cinq ans pour une stratégie en matière de cybersécurité, ce que j'ai compris, c'est que vous bâtissiez un cadre, une organisation bureaucratique et que vous déterminiez les rôles de chacun en la matière. Est-ce qu'une partie des fonds sera consacrée aux outils, à l'équipement et à la surveillance ou est-ce que les fonds serviront uniquement à établir le cadre?

**Mme Merchant :** En ce qui a trait à la stratégie, il y a deux volets : il y a la stratégie en soi, qui énonce les trois objectifs à atteindre, et il y a le financement associé aux initiatives en vue de réaliser la stratégie.

**La sénatrice Wallin :** Donnez-moi un exemple.

**Mme Merchant :** Des initiatives? Le centre cybernétique ou l'Unité nationale de coordination de la lutte contre la cybercriminalité.

**Senator Wallin:** Are those funded? When you have a unit, does the money actually pay salaries, buy equipment? I'm trying to see where that money actually goes.

**Mr. Adam:** The funding for the national coordination unit will need an IM/IT infrastructure behind it so that the public can report the cybercrime in an easy, public-facing fashion. We will need the analytics behind that, which will then drive how we respond.

Right now, we have no idea what's happening across Canada, for example. To be able to coordinate what is going on in Canada with our international allies that say, "Are you having this problem?" and we say, "Maybe", we don't know, and we try to find out.

Part of the money coming to the RCMP will be in support of cyber investigative teams. It's proposed that we'll have two —

**Senator Wallin:** These are actual people with paycheques?

**Mr. Adam:** These are people with paycheques, comprised of investigators, and technical expertise which comes from the technical operations world. So there is a law enforcement response built into this.

**Senator Wallin:** I ask about that, because I want to come back to the question we were discussing with our earlier witness today, which is who should be responsible for this. I will put the question this way: Can the Canadian government afford to secure itself and protect Canadians against security threats?

I know we don't really know the degree of the threat, but how do you fund that? When you look at Facebook losing $50 billion in 48 hours and then you look at $108 million, we're not in the same league. Can it be government's job, and if so, how would that possibly be funded?

**Ms. Merchant:** In terms of the funding, I'd like to have an answer for that myself. But in terms of whether the government can do all of this, absolutely not. The federal government can't, and that's why partnerships are so important. And it's not just partnerships — federal government to provinces and territories or federal government to the private sector, critical infrastructure owners and operators — it's amongst all of us.

What we heard from the review was that these organizations or these entities are looking for a leader. Who is going to be the force multiplier? Who is going to get out there and figure out the best partnerships, the best way to connect the needs with those

**La sénatrice Wallin :** Est-ce qu'ils sont financés? Lorsque vous avez une unité, est-ce que les fonds couvrent les salaires et l'équipement? J'essaie de comprendre où iront les fonds.

**M. Adam :** Pour le financement de l'unité nationale de coordination, il faudra une infrastructure de GI/TI de sorte que la population puisse dénoncer la cybercriminalité facilement. Nous aurons besoin d'analyses, qui orienteront notre manière d'intervenir.

À l'heure actuelle, nous n'avons aucune idée de ce qui se passe au Canada, par exemple. Ce serait bien de pouvoir coordonner ce qui se passe au Canada avec nos alliés internationaux pour tenter de comprendre les problèmes et de les régler.

Une partie des fonds octroyés à la GRC servira aux équipes spécialisées en matière de cyberenquête. On propose d'établir deux…

**La sénatrice Wallin :** Ce sont des gens, qui reçoivent un chèque de paie?

**M. Adam :** Oui. Ce sont notamment des enquêteurs, des gens qui ont une expertise technique, qui viennent du domaine des opérations techniques. On intègre donc le volet d'intervention en matière d'application de la loi.

**La sénatrice Wallin :** Je vous en parle parce que je veux revenir à la question dont nous avons discuté avec notre témoin précédent, c'est-à-dire : qui est responsable? Je vais formuler la question ainsi : le gouvernement canadien a-t-il les moyens de se protéger et de protéger les Canadiens contre les menaces en matière de sécurité?

Je sais que nous ne savons pas quel est le degré de cette menace, mais comment est-ce qu'on finance cela? Lorsqu'on pense à Facebook, qui a perdu 50 milliards en 48 heures et qu'on pense ensuite à ces 108 millions de dollars… Ce n'est pas du tout la même catégorie. Est-ce que le gouvernement peut s'acquitter de cette tâche et, dans l'affirmative, comment financerait-on cela?

**Mme Merchant :** En ce qui a trait au financement, j'aimerais connaître la réponse. Mais en ce qui a trait à la capacité du gouvernement de faire tout cela, la réponse est claire : il n'a pas cette capacité. C'est pour cela que les partenariats sont si importants. Et il n'y a pas seulement les partenariats entre le gouvernement fédéral et les provinces et les territoires, ou entre le gouvernement fédéral et le secteur privé, les propriétaires d'infrastructures essentielles et les exploitants; nous avons tous un rôle à jouer à cet égard.

Ce que nous avons compris de l'examen, c'est que ces organisations ou ces entités cherchent un responsable. Qui sera le multiplicateur de force? Qui sera responsable d'établir les meilleurs partenariats, les meilleures façons de jumeler les

who can supply some of the answers? Obviously that's kind of the step that we're taking with the new cybersecurity strategy.

**Mr. Boucher:** If I may add to this. The government has a responsibility to protect itself today and it is doing so. There is already a large amount of money being spent protecting the government.

This money helps us bring together those pieces and create that efficiency and effectiveness that perhaps we could do better at, and not become victims and not make the news like private sector companies have done this week.

So these numbers are not the only numbers, and it's important to remember that.

**Senator Wallin:** I realize that. But you're talking about protecting government, and I did have a second part of the question which you can answer in the course of other questions, which is: What about Canadians?

[*Translation*]

**Senator Dagenais:** I have a supplementary question for Mr. Adam about budgets. Over the past five years, the RCMP has inherited a number of mandates, including the fight against terrorism and cybercrime. Can you give us an overview of the change in your staff over the past five years and in the number of individuals who will be mobilized in the cybercrime file? You are relocating staff to use some people to fight cybercrime and others to fight terrorism.

The investigations unit can be overlooked because I assume it requires more people and a bigger budget. Are you being given a bigger budget and more employees, or are you only relocating people, which may inadvertently lead to some files being overlooked?

[*English*]

**Mr. Adam:** It's a well-known fact we are in the hole on investigators. We are recruiting as fast as we can to maintain the level which we are funded at. There will never ever be enough money for police to catch every single criminal, every single speeder; not possible.

So we, within the RCMP, must prioritize our activities based to the greatest threats to both public safety and to Canadians including the economy.

There have been times where we have had to respond in one direction, trying to leverage and average those out. In this case, this is not just for the RCMP, although the funding is directed at

besoins aux personnes qui peuvent y répondre? C'est la voie que nous voulons suivre avec la nouvelle stratégie en matière de cybersécurité.

**M. Boucher :** Si je peux ajouter quelque chose, le gouvernement est actuellement responsable de se protéger, et c'est ce qu'il fait. On consacre déjà d'importantes sommes à la protection du gouvernement.

Cet argent nous aidera à regrouper les éléments et à accroître notre efficacité, afin de ne pas devenir des victimes et de ne pas faire les manchettes, comme cela a été le cas de certaines entreprises du secteur privé cette semaine.

Ce ne sont donc pas uniquement des chiffres; il ne faut pas l'oublier.

**La sénatrice Wallin :** Je comprends. Mais vous parlez de protéger le gouvernement et il y avait une autre partie à ma question, à laquelle vous pourrez peut-être répondre plus tard : qu'en est-il des Canadiens?

[*Français*]

**Le sénateur Dagenais :** J'ai une question complémentaire à poser à M. Adam concernant les budgets. Depuis les cinq dernières années, la GRC a hérité de plusieurs mandats, y compris la lutte au terrorisme et à la cybercriminalité. Pouvez-vous nous dresser un tableau de l'évolution de vos effectifs depuis les cinq dernières années et du nombre de personnes qui vont être mobilisées en ce qui a trait à la cybercriminalité? Si vous prenez des personnes pour combattre la cybercriminalité, et d'autres pour combattre le terrorisme, c'est parce que vous déplacez des effectifs.

Le service des enquêtes peut être négligé, parce que j'imagine qu'il nécessite plus de personnes et un budget plus important. Est-ce qu'on vous donne un plus gros budget et plus d'employés, ou est-ce que vous déplacez seulement des gens, ce qui, malencontreusement, peut faire en sorte que d'autres dossiers soient négligés?

[*Traduction*]

**M. Adam :** C'est bien connu : nous n'avons pas assez d'enquêteurs. Nous les recrutons le plus vite possible afin de maintenir un niveau correspondant à notre financement. Il n'y aura jamais assez d'argent pour permettre aux policiers d'attraper tous les criminels, tous les gens qui font des excès de vitesse… c'est impossible.

La GRC doit donc établir l'ordre des priorités en fonction des plus grandes menaces pour la sécurité publique et pour les Canadiens, y compris l'économie canadienne.

À certains moments, nous avons dû intervenir de manière unidirectionnelle et tenter de miser sur ce que nous avions. Dans le cas présent, il ne s'agit pas seulement de la GRC, bien que le

the RCMP at this time. I am currently the chair of the Canadian Association of Chiefs of Police's Electronic Crime Committee. One of the subcommittees reporting to me is cyber, so that is the law enforcement of Canada trying to figure out how to address cyber, right to the detachment grassroots level. And it is not necessarily a new type of crime, like terrorism was. This is a new way criminal activity is happening.

While it may appear if you turn your head and think of cyber as a thing, most of the criminality is just using cyber vectors to conduct their criminal activities. It's not really a change in how or what we're doing, it's a change in how we're doing it. Some other initiatives we are looking at are — and I speak frankly — do I need a gun to investigate cybercrime? Frankly, it's nice to have, but I don't need one.

We are looking at changing how we do business on that investigative frontier where the perpetrators could be anywhere in the world and they may be, for all intents and purposes, kids that have never left the basement of their mother's house.

So we have to change how we look at how we investigate, who we investigate with, and what is the outcome of an investigation. To answer your question the long way, we're getting two new teams, new analysts and new abilities to analyze what's happening, to direct our efforts in the best way we can.

[*Translation*]

**Senator Dagenais:** Is anything set aside in Budget 2018 for your staff?

[*English*]

**Mr. Adam:** What we got was, in part, what we asked for.

**Senator Tkachuk:** I just have a couple of questions. Ms. Merchant and Mr. Boucher, do you have a background in cybersecurity?

**Ms. Merchant:** My academic background is in aerospace engineering and I have a graduate degree in theoretical physics. However, I have worked in cybersecurity for many years.

**Mr. Boucher:** Thank you for the question. I have a bachelor's degree in computer science, a master's degree in software engineering, a graduate degree in defence studies. I spent 32 years in the military, of which the last 15 years have been focused on cybersecurity.

I've been in the Communications Security Establishment for five years.

financement lui soit octroyé. Je suis président du comité de l'Association canadienne des chefs de police sur le crime électronique. Le sous-comité sur la cybercriminalité relève de moi. Les agents de l'application de la loi tentent donc de trouver des façons de lutter contre la cybercriminalité, et ce à partir de la base, au niveau du détachement. Il ne s'agit pas nécessairement d'un nouveau type de crime, comme l'était le terrorisme. Il s'agit d'une nouvelle façon de s'adonner à des activités criminelles.

Bien qu'on puisse penser que la cybercriminalité est un monde en soi, la plupart des criminels se servent uniquement de vecteurs cybernétiques pour réaliser leurs activités. Cela ne change pas vraiment ce que nous faisons, mais plutôt la façon dont nous faisons les choses. On revoit certaines choses, notamment — et je parle franchement ici — la nécessité d'avoir un fusil pour faire enquête sur la cybercriminalité. Bien honnêtement, je préfère en avoir un, mais je n'en ai pas besoin.

Nous songeons à changer nos méthodes d'enquête, puisque les criminels peuvent se trouver n'importe où dans le monde. Ils peuvent même être des jeunes qui n'ont jamais quitté le sous-sol de leurs parents.

Il faut donc changer notre vision quant à la façon d'enquêter, aux personnes avec qui nous collaborons et aux résultats des enquêtes. Pour répondre à votre question en détail, nous allons créer deux nouvelles équipes, recruter de nouveaux analystes et avoir de nouvelles capacités pour analyser ce qui se passe et diriger nos efforts le mieux possible.

[*Français*]

**Le sénateur Dagenais :** Y a-t-il quelque chose qui est prévu dans le budget de 2018 pour vos effectifs?

[*Traduction*]

**M. Adam :** Nous avons obtenu ce que nous avions demandé, en partie.

**Le sénateur Tkachuk :** J'aimerais vous poser quelques questions. Madame Merchant, monsieur Boucher, avez-vous une expérience en matière de cybersécurité?

**Mme Merchant :** J'ai étudié le génie aérospatial et j'ai un diplôme d'études supérieures en physique théorique. Je travaille toutefois dans le domaine de la cybersécurité depuis de nombreuses années.

**M. Boucher :** Je vous remercie de votre question. J'ai un baccalauréat en informatique, une maîtrise en génie logiciel et un diplôme d'études supérieures en études de la défense. J'ai passé 32 ans dans l'armée, dont 15 ans à travailler dans le domaine de la cybersécurité.

Je travaille au Centre de la sécurité des télécommunications depuis cinq ans.

**Senator Tkachuk:** You have no idea how that makes me feel better. I'm a little confused because Ms. Merchant is the director general of the National Cyber Security Directorate, and then we have the Communications Security Establishment.

Are you interrelating? Who is the boss? Who is in charge of all this? Are you in charge? Is Ms. Merchant in charge?

**Ms. Merchant:** "In charge" is a very loose term. In the Canadian government, I really honestly believe that it works better inside than it looks like from the outside. There are at least 14 departments and agencies with a direct influence or responsibility related to cybersecurity, so it depends on each minister's mandate and their responsibilities under the relative acts of the ministries. But Public Safety has been accorded the responsibility to coordinate amongst those departments and agencies, and also externally within the private sector as required in the event of an incident.

So both for policy matters and for operational incident matters, we have a coordinating role at this point in time. And I say "at this point in time" because for the operational piece, incident management piece, that will transfer to the centre when it is created.

**Senator Tkachuk:** I don't know for sure if there is, and you're going to tell me, but is there a unit in Canada Revenue? There are probably people interested in cybersecurity in CPP, I would think, where personal information can potentially be taken, or perhaps National Defence. Is that kind of the way it's structured ?

**Ms. Merchant:** How it is structured, in general, is every department is responsible for the securing its sensitive information, personal information they're dealing with and that's dealt with through the Office of the Privacy Commissioner.

In terms of cybersecurity, there are departments. We have 10 critical infrastructure sectors and there are departments who have a responsibility for those critical infrastructure sectors, for example, Transport Canada for transportation, Natural Resources Canada for energy and so on. So those 10 departments are interested in cybersecurity from a critical infrastructure perspective.

In addition, you've got departments such as Global Affairs where they have a vested interest. For example, the Budapest convention on crime that Jeff had mentioned is something that is international. We want like-minded countries to gather and be a part of this so that we can work internationally. Global Affairs would be responsible for those types of things.

**Le sénateur Tkachuk :** Vous n'avez pas idée à quel point cela me rassure. Je suis un peu perdu parce que Mme Merchant est la directrice générale de la Direction de la cybersécurité nationale et nous avons aussi le Centre de la sécurité des télécommunications.

Êtes-vous liés l'un à l'autre? Qui est le patron? Qui est responsable de tout cela? Est-ce vous? Est-ce que c'est Mme Merchant?

**Mme Merchant :** Le mot « responsable » est assez vaste. Je crois que le gouvernement du Canada fonctionne mieux à l'intérieur que ce qu'il en paraît à l'extérieur. Il y a au moins 14 ministères et organismes qui ont une incidence ou une responsabilité directe à l'égard de la cybersécurité; cela dépend donc du mandat de chaque ministère et de leurs responsabilités en vertu des lois qui s'appliquent à eux. On a toutefois accordé à Sécurité publique la responsabilité de coordonner ces ministères et organismes et aussi de coordonner le travail avec le secteur privé selon les besoins en cas d'incident.

Ainsi, à l'heure actuelle, nous assurons un rôle de coordination tant pour les questions de politiques que pour les questions relatives aux incidents opérationnels. Et je dis « à l'heure actuelle » parce que le volet opérationnel et le volet de gestion des incidents seront transférés au centre lorsqu'il sera créé.

**Le sénateur Tkachuk :** Je ne sais pas si cela existe, et vous allez me le dire, mais est-ce qu'il y a une unité au sein de l'Agence du revenu du Canada? Il y a certainement des gens qui s'intéressent à la cybersécurité au RPC, d'après moi, car on peut y prendre des renseignements personnels, ou peut-être à la Défense nationale. Est-ce un peu ainsi que c'est structuré?

**Mme Merchant :** Selon la façon dont c'est structuré en général, chaque ministère a la responsabilité de veiller à la sécurité de ses renseignements délicats et des renseignements personnels qu'il traite, et cela se fait par l'intermédiaire du Commissariat à la protection de la vie privée.

Pour ce qui est de la cybersécurité, il y a des ministères. Nous avons 10 secteurs des infrastructures essentielles, et ce sont des ministères qui assument une part de responsabilités de ces secteurs des infrastructures essentielles, par exemple, Transports Canada pour le transport, Ressources naturelles Canada pour l'énergie, et ainsi de suite. Donc, ces 10 ministères s'intéressent à la cybersécurité dans l'optique des infrastructures essentielles.

De plus, vous avez des ministères qui ont un intérêt particulier, comme Affaires mondiales Canada. Par exemple, la Convention de Budapest sur la criminalité, que Jeff a mentionnée, a une portée internationale. Nous voulons que les pays partageant les mêmes vues se réunissent et fassent partie de cela, de sorte que nous puissions travailler à l'échelle internationale. Affaires mondiales assumerait la responsabilité de ce genre de choses.

Then we have the Department of National Defence, which is responsible for the military aspects of cybersecurity, both domestically and internationally and the Communications Security Establishment, for example. There are many departments involved from many different perspectives and it does require a close coordination.

**Senator Tkachuk:** What do you see as the greatest threat? Is it domestic, is it foreign governments? Where do you think the greatest threat is to attacking government systems? We've had a lot of debate about this. There has to be something that worries you guys and that you spend a lot of time on.

**Mr. Boucher:** There are a lot of things that worry us. If I complement Colleen's description, at the operational level you have a number of departments protecting themselves, defending themselves, integrated together. Most are under the umbrella of Shared Services, which is also monitoring and defending themselves, and wrapping this together is CSE, monitoring and detecting for bad actors.

I would say our biggest threat frankly is — but we're about to fix it — the seams between these entities. There are a lot of seams and entities and currently we are exposed because of these seams, and the more we bring these seams together, the less exposed we are and the more we have a bubble we create, and a better chance we have to detect and respond.

Who are the threat actors of concern? There is a myriad of threat actors and we have to characterize them to better understand their attitudes and how they will operate, what they are interested in, their likely motivations. They range from the basement kids who want to show their friends that they can, all the way to state actors who are well organized and well resourced.

In the range between these two entities is a spectrum including cybercriminals, those activists who are motivated by a vision of the world that is alternative to ours, so all of these have not only different intent but capacities. But I would say we are worried because many of these negative cybercapacities are becoming commercially available. You do not have to be as sophisticated as you used to be able to create a grave impact.

**Senator Wetston:** To follow up on Senator Tkachuk, there are a lot of seams in the country, not just federally, and what are you able to accomplish when all of the provinces are also dealing with cybersecurity issues? How do you propose to interface with the provinces? And, of course, Mr. Adam, you obviously need to do that regularly on a law enforcement basis.

Puis nous avons le ministère de la Défense nationale, qui est responsable des aspects militaires de la cybersécurité, tant au Canada qu'à l'étranger, et le Centre de la sécurité des télécommunications, par exemple. De nombreux ministères interviennent sous divers angles et il faut pour cela une étroite coordination.

**Le sénateur Tkachuk :** Qu'est-ce qui représente la plus grande menace, à votre point de vue? Vient-elle du Canada ou de gouvernements étrangers? D'après vous, d'où vient la plus grande menace d'attaques contre les systèmes gouvernementaux? Nous avons beaucoup débattu de cela. Il doit bien y avoir des choses qui vous inquiètent et auxquelles vous consacrez beaucoup de temps.

**M. Boucher :** Bien des choses nous inquiètent. Pour ajouter à la description de Colleen, à l'échelon opérationnel, vous avez divers ministères qui se protègent eux-mêmes, qui se défendent eux-mêmes, et qui sont intégrés ensemble. La plupart sont regroupés sous l'égide de Services partagés, qui se défend aussi lui-même et assure sa propre surveillance, puis vous avez pour l'ensemble le CST, qui exerce une surveillance et travaille à détecter les acteurs malveillants.

Franchement, je dirais que notre plus grande menace — que nous sommes sur le point de régler — se situe aux points de jonction entre ces entités. Il y a beaucoup de points de jonction et d'entités, et nous sommes exposés, en ce moment, à cause de cela. Plus nous scellons ces points jonctions, moins nous serons exposés, plus nous serons dans une bulle, et mieux nous serons en mesure de détecter les problèmes et d'y répondre.

Qui sont les acteurs malveillants qui nous préoccupent? Il y en a une myriade, et nous devons mieux les caractériser afin de mieux comprendre leurs attitudes et la façon dont ils vont fonctionner, ce qui les intéresse, et ce qui les motive vraisemblablement. Ils vont du jeune dans son sous-sol qui veut montrer ce qu'il peut faire à ses amis à l'acteur étatique qui est bien organisé et doté d'excellentes ressources.

Entre ces deux extrêmes, il y a toute une gamme d'acteurs, dont le cybercriminel et le militant motivé par une vision du monde différente de la nôtre. Ils ont tous des intentions différentes, mais aussi des capacités différentes. Je dirais cependant que nous sommes préoccupés parce que bon nombre de ces cybercapacités négatives sont de plus en plus offertes sur le marché. Vous n'avez pas besoin d'un aussi grand raffinement qu'avant pour produire de graves conséquences.

**Le sénateur Wetston :** Je vais poursuivre dans la même veine que le sénateur Tkachuk. Il y a beaucoup de points de jonction au pays, pas juste à l'échelon fédéral. Qu'est-ce que vous êtes en mesure d'accomplir, alors que toutes les provinces doivent aussi s'occuper de questions de cybersécurité? Que proposez-vous comme interface avec les provinces? Bien sûr, monsieur Adam, vous devez manifestement le faire régulièrement par l'application de la loi.

Can you give me insight as to how this strategy, in some way or another, might assist, influence the ability of the provinces to also be able to respond to cybersecurity threats?

**Ms. Merchant:** Within Public Safety Canada, since we do this broad coordination role, we have what we call "sector networks." I will start small. We start with a sector, and this is where we get together with members of the federal government, provinces and territories and the private sector, within that sector, to exchange information and make best use of all the collective knowledge within that sector.

We also have a multi-sector forum where we gather all 10 of the critical infrastructure sectors— the federal government, provinces and territories and the private sector— so that between the sectors they can share information and best practices. Our deputy minister is a co-chair of the national cross-sector forum, which gets together the CEOs of associations representing all 10 sectors; so in a more formalized fashion is how we work together.

In something that's much more optional, public safety houses, the Canadian Cyber Incident Response Centre, CSIRC, and they came in October and talked to this committee.

CSIRC has partnerships with provinces and territories with critical infrastructure. That is a construct. It is a one-stop shop where they can not only report incidents or provide, in an anonymous way, malware or problems on their network where it is anonymized and then CSIRC is able to issue reports or alerts or warnings to the broad partnership, which is over 1,200 various entities.

There are operational mechanisms to share information on short notice such that the whole community can deal with incidents, issues or threats. Then there is a more formalized way to get up through the management structure, the bureaucratic structure, of all of the provinces, territories and critical infrastructure sectors.

**Mr. Boucher:** Take CSIRC and the experts in the federal government, bring them together in a cyber centre, a new place, where you open your doors— and it goes to Senator Wallin's question— to private sector entities, to Canadians, citizens, to small firms, and you can share this knowledge about cybersecurity, about the threat and the measures you can take and sharing that expertise and create the workforce and the tools and do it together.

Pouvez-vous me donner une idée de la façon dont cette stratégie pourrait, d'une manière ou d'une autre, influencer la capacité des provinces d'être aussi en mesure de répondre aux menaces à la cybersécurité?

**Mme Merchant :** Au sein de Sécurité publique Canada, depuis que nous assumons ce vaste rôle de coordination, nous avons ce que nous appelons des « réseaux sectoriels ». Je vais commencer par le plus petit élément. Nous commençons par un secteur, et nous nous réunissons avec les membres du gouvernement fédéral, des provinces, des territoires et du secteur privé au sein de ce secteur, afin d'échanger de l'information et de tirer le maximum de toutes les connaissances collectives de ce secteur.

Nous avons aussi un groupe de discussion multisectoriel où nous réunissons les 10 secteurs des infrastructures essentielles — au sein du gouvernement fédéral, des provinces et territoires et du secteur privé —, de sorte qu'il y a un échange de renseignements et de pratiques exemplaires entre les secteurs. Notre sous-ministre copréside le groupe de discussion multisectoriel national, qui rassemble les PDG des associations représentant les 10 secteurs. C'est donc ainsi que nous travaillons ensemble d'une manière plus formelle.

Dans un cadre beaucoup plus optionnel, on trouve au sein de Sécurité publique Canada le Centre canadien de réponse aux incidents cybernétiques, le CCRIC, dont les représentants ont comparu devant le comité en octobre.

Le CCRIC a des partenariats avec les provinces et territoires comportant des infrastructures essentielles. C'est un concept. C'est un guichet unique où les gens peuvent non seulement signaler les incidents ou signaler anonymement des logiciels malveillants ou des problèmes sur leur réseau. L'information est anonymisée, et le CCRIC est en mesure de transmettre des rapports, des alertes ou des avertissements à l'ensemble des membres du partenariat, soit à plus de 1 200 entités diverses.

Il y a des mécanismes opérationnels servant à diffuser très rapidement l'information de sorte que toute la communauté puisse faire face aux incidents, aux problèmes ou aux menaces. Il y a aussi une façon plus officielle de passer par la structure de gestion, la structure bureaucratique, de l'ensemble des provinces, territoires et secteurs des infrastructures essentielles.

**M. Boucher :** Prenez le CCRIC et les experts du gouvernement fédéral, rassemblez-les dans un centre cybernétique — et cela est lié à la question de la sénatrice Wallin —, un nouveau lieu dont vous ouvrez les portes aux entités du secteur privé, aux Canadiens, aux citoyens et aux petites entreprises, et vous pouvez diffuser ces connaissances sur la cybersécurité, sur les menaces et les mesures que vous pouvez prendre, transmettre cette expertise, créer l'effectif et les outils, et travailler ensemble.

That's the vision of the cyber centre where we create this place to bring these folks together.

**Senator Wetston:** We have heard from other witnesses who we are a bit behind in the establishment of this kind of centre. I will not ask you to comment because you will probably disagree, but that's fine. Read the transcripts.

Is CSIS excluded from the national cybersecurity strategy? Are they getting any of this largess being spread among the entities before us today? According to Senator Stewart Olsen, it is not enough money. We have heard that.

**Ms. Merchant:** Aside from what has already been announced in the budget, we have to wait to see what further detailing there is within the funding that was allocated to other initiatives.

**Senator Wetston:** Chief superintendent, have you ever prosecuted anyone in this space yet, for cybersecurity?

**Mr. Adam:** Yes, I have.

**Senator Wetston:** Has there been a significant number?

**Mr. Adam:** When I was prosecuting in New Brunswick, and working as the first member in the Atlantic provinces of the Technological Crime Unit— that was me— and Mr. Cabana was in Proceeds of Crime at the time.

**Senator Wetston:** I did some work with him.

**Mr. Adam:** Excellent. My time there was just a couple of years before I moved out. Most of my work was about digital forensic recovery in support of other crimes, or to get evidence off of computers. However, there were two cases that I'm aware where it was a hacker selling passwords and the other one was someone who had wiped out a web space of a company in the States.

**Senator Wetston:** Thank you very much.

**Senator Ringuette:** The half billion dollars— you've talked about sharing knowledge and so forth— are you going to have a portion of these funds leveraged with the private sector for research purposes?

**Ms. Merchant:** For us that comes through our grants and contributions program, which is open to provinces, territories, the private sector and academia.

C'est la vision du centre cybernétique: la création d'un lieu qui rassemble ces gens.

**Le sénateur Wetston :** Nous avons entendu d'autres témoins qui accusent un peu de retard dans l'établissement de ce type de centre. Je ne vous demanderai pas vos observations, car vous ne serez probablement pas d'accord, mais ça va. Lisez les transcriptions.

Le SCRS est-il exclu de la Stratégie nationale de cybersécurité du Canada? Est-ce qu'il profite d'une partie de cette largesse dont profitent les entités qui sont devant nous aujourd'hui? Selon la sénatrice Stewart Olsen, ce n'est pas assez d'argent. Nous avons entendu cela.

**Mme Merchant :** Outre ce qui a déjà été annoncé dans le budget, nous devons attendre les détails relatifs aux fonds qui ont été affectés à d'autres initiatives.

**Le sénateur Wetston :** Surintendant principal, avez-vous déjà poursuivi quelqu'un dans cet espace, en matière de cybersécurité?

**M. Adam :** Oui.

**Le sénateur Wetston :** Est-ce qu'il y a eu beaucoup de cas?

**M. Adam :** Quand je m'occupais de poursuites au Nouveau-Brunswick, et en tant que premier membre du Groupe de la criminalité technologique dans les provinces de l'Atlantique — c'était moi —, M. Cabana était aux produits de la criminalité.

**Le sénateur Wetston :** J'ai eu l'occasion de travailler avec lui.

**M. Adam :** Excellent. Je n'y ai passé que deux ans avant de partir. L'essentiel de mon travail était la recherche d'éléments de preuve informatique à l'appui d'autres crimes, c'est-à-dire trouver des preuves dans les ordinateurs. Cependant, je suis au courant de deux cas, dont un pirate informatique qui vendait des mots de passe et un individu qui avait fait disparaître l'espace web d'une société aux États-Unis.

**Le sénateur Wetston :** Merci beaucoup.

**La sénatrice Ringuette :** Concernant le demi-milliard de dollars — vous avez parlé de diffusion des connaissances et ainsi de suite —, allez-vous miser sur le secteur privé pour une partie de ces fonds à des fins de recherche?

**Mme Merchant :** Dans notre cas, cela vient de notre programme de subventions et de contributions, qui est ouvert aux provinces, aux territoires, au secteur privé et au milieu universitaire.

**Senator Ringuette:** The purpose of creating this bubble and this communication of knowledge and problem issues, could you not use that as a trigger point for developing funding research for that problem issue as you move along?

[*Translation*]

**Mr. Boucher:** That is already being done now. At CSE, we are already encouraging private partnerships. The issue is not about finding resources, but about finding and correctly identifying the problem and bringing together academics.

**Senator Ringuette:** So what you are creating should help you identify the problem.

**Mr. Boucher:** Yes.

**Senator Ringuette:** Okay.

[*English*]

We have Health Canada that labels what is in the food that we consume. We have the electrical stuff, the CSA, with the appliances that we use. Is there any project in Canada to help Canadian consumers when they buy phones or laptops, a rating system in respect to cybersecurity?

**Ms. Merchant:** There is an entity in New Brunswick called Cyber New Brunswick, and they have promoted something called "cyber essentials." I believe it is starting to get off the ground. It's a way in which companies or manufacturers can have a certification applied to their product.

**Senator Tkachuk:** I think she knew that.

**Senator Ringuette:** You can understand the synergy I have with my constituency, though.

**Ms. Merchant:** Yes. I want to mention that is something, as I had mentioned in my notes, we had heard through the review is that there is a desire for legislation, standards or guidelines that would help consumers and would help the accessibility of these products to consumers. That's something we are aware of and taking into consideration.

**Senator Ringuette:** Into consideration to do what?

We're talking about cybersecurity for government apparatus and the private sector, but the citizens out there and consumers of these Wi-Fi products and all the technical gadgets that we buy.

**Ms. Merchant:** ISED is very interested in this particular topic.

**La sénatrice Ringuette :** Pour l'objectif de créer une bulle, de diffuser les connaissances et de fournir des renseignements sur les problèmes et enjeux, ne pourriez-vous pas utiliser cela comme point de déclenchement pour développer le financement des recherches à l'avenir, pour ces problèmes et enjeux?

[*Français*]

**M. Boucher :** On le fait déjà aujourd'hui. Au CST, on favorise déjà des partenariats privés. Le problème, ce n'est pas de trouver les ressources, mais de trouver et de cerner le bon problème et de réunir les gens de l'académie.

**La sénatrice Ringuette :** Donc, ce que vous êtes en train de créer devrait vous aider à cerner le problème.

**M. Boucher :** Oui, madame.

**La sénatrice Ringuette :** D'accord.

[*Traduction*]

Nous avons Santé Canada qui étiquette ce qu'il y a dans la nourriture que nous consommons. Nous avons les trucs électriques, les normes CSA, pour les appareils que nous utilisons. Est-ce qu'on envisage de créer quelque chose au Canada pour aider les consommateurs canadiens lors de l'achat de téléphones ou d'ordinateurs portatifs — un système de cote pour la cybersécurité?

**Mme Merchant :** Il existe au Nouveau-Brunswick une entité appelée CyberNB, et elle fait la promotion de la norme Cyber Essentials. Je crois que c'est en train de prendre son envol. Cela permet aux sociétés ou aux fabricants d'obtenir la certification de leurs produits.

**Le sénateur Tkachuk :** Je crois qu'elle le savait.

**La sénatrice Ringuette :** Vous voyez la synergie que j'ai avec ma circonscription.

**Mme Merchant :** Oui. Je veux souligner, comme je l'ai mentionné dans mes notes, que l'examen nous a permis d'entendre que les gens souhaitent des mesures législatives, des normes ou des lignes directrices qui aideraient les consommateurs, notamment à accéder à ces produits. C'est une chose dont nous sommes au courant et dont nous tenons compte.

**La sénatrice Ringuette :** À quelle fin?

Nous parlons de cybersécurité pour l'appareil gouvernemental et le secteur privé, mais il y a les citoyens et les consommateurs de ces produits sans fil et de tous les gadgets technologiques que nous achetons.

**Mme Merchant :** Ce sujet en particulier est d'un grand intérêt pour ISDE.

**Senator Ringuette:** Are they part of your bubble?

**Ms. Merchant:** Which bubble?

**Senator Ringuette:** Mr. Boucher's bubble.

[*Translation*]

**Mr. Boucher:** They are definitely among the people with whom we develop great ideas we mean to use to move forward. The problem is that some things may still be in development and have not been announced yet. We will have more material to provide over the coming months. These types of ideas are definitely at the forefront of our discussions.

**Senator Dagenais:** I have a second question for Mr. Adam. Just before you, a specialist from the University of Waterloo talked to us about very interesting and advanced research being conducted at the university. If I was a hacker, why wouldn't I enrol as a student at the University of Waterloo to stay abreast of what is happening? Are any security actions performed to avoid the piracy of our knowledge and of what is being taught at universities?

[*English*]

**Mr. Adam:** We have trouble security clearing our own folks without considering university students.

In fairness, I would hope the universities are cognizant of the students to which they give some of this information, but frankly I think if they are registered at the university then, frankly, they should have access.

We, like our partners, also engage universities to do research projects, but we do security clear the students. We do work with the instructors and we do partition the information that the student gets access to. There is no guarantee ever of anyone not going *pirate*, but our experience has not been that that's the case. There is nothing to stop anyone from learning anything, anywhere and then using it for criminal ends.

[*Translation*]

**Senator Dagenais:** Thank you, Mr. Adam.

[*English*]

**Senator Marwah:** It's really quite reassuring to hear all the activities that are taking place, but I think each of you have mentioned this is a highly evolving and rapidly developing space. Given that, how do you fight the war for talent? All the kids want to go work for start-ups or Google or Facebook, notwithstanding their problems.

**La sénatrice Ringuette :** Ce ministère se trouve-t-il dans votre bulle?

**Mme Merchant :** Quelle bulle?

**La sénatrice Ringuette :** La bulle de M. Boucher.

[*Français*]

**M. Boucher :** Ils font définitivement partie des gens avec qui on élabore les grandes idées avec lesquelles on prévoit aller de l'avant. La difficulté, c'est que certaines choses sont peut-être en cours d'élaboration et n'ont pas encore été annoncées. On aura plus de matériel à offrir au cours des mois à venir. Ce genre d'idées est certainement au centre de nos discussions.

**Le sénateur Dagenais :** J'ai une deuxième question qui s'adresse à M. Adam. Juste avant vous, un spécialiste de l'Université de Waterloo nous a parlé de travaux de recherche qui sont menés à l'université et qui sont très intéressants et très avancés. Si je suis un pirate, pourquoi ne m'inscrirais-je pas comme étudiant à l'Université de Waterloo afin d'être bien informé de ce qui se fait? Y a-t-il des actions de sécurité qui sont menées afin d'éviter le piratage de nos connaissances et de ce qu'on enseigne dans les universités?

[*Traduction*]

**M. Adam :** Nous avons déjà de la difficulté à vérifier nos propres gens, sans nous occuper des étudiants universitaires.

Franchement, j'espère que les universités connaissent les étudiants auxquels elles donnent de tels renseignements, mais d'après moi, les étudiants qui sont inscrits à l'université devraient y avoir accès.

À l'instar de nos partenaires, nous utilisons les universités pour la réalisation de projets de recherche, mais nous soumettons les étudiants à des vérifications de sécurité, en pareils cas. Nous travaillons avec les instructeurs, et nous cloisonnons l'information à laquelle les étudiants ont accès. Il n'y a aucune garantie, car n'importe qui peut devenir pirate, mais nous n'avons pas vécu cela. Rien ne peut empêcher quiconque d'apprendre ce qu'il veut, où il veut, puis d'utiliser ses connaissances à des fins criminelles.

[*Français*]

**Le sénateur Dagenais :** Merci, monsieur Adam.

[*Traduction*]

**Le sénateur Marwah :** C'est vraiment très rassurant d'entendre tout ce qui se fait, mais je crois que chacun de vous a signalé que c'est un espace en évolution très constante et rapide. Compte tenu de cela, comment vous battez-vous pour l'emporter dans la chasse aux talents? Tous les jeunes veulent travailler

Another way to put it is: What percentage of your budgets would be recruitment, training and research so you can keep abreast of what is going on?

**Mr. Boucher:** I can certainly start for CSE, because we have on-the-ground experience today.

It should not surprise you that Canadians are driven by things other than money. So the appeal of start-ups and the appeal of a life on the West Coast of any country certainly attracts an individual, but the noble cause of being here, defending the nation and ensuring the security and safety of Canadians also attracts some back.

It is CSE's experience we do lose some really good talent at times. I'm proud to say that often times they do come back because the appeal of working for someone else's revenue quickly fades and once you have the sports car and the nice apartment, you realize you are lacking meaning in life. They literally come back.

This is a point of success, today. I won't lie; it is a constant challenge and we need to keep offering a place of employment that is attractive to young people, that adapts to the changing cultures of the younger generations, that keeps pace with technology and offers constant training and so on, and I think you are very much aware of that. It is on us to offer the environment. I apologize, I do not have the numbers for how much we resource this effort.

**Senator Marwah:** Is it a small, medium or large number? Is there any sense? Would it be 5 per cent of your budget, or 25 per cent?

**Mr. Boucher:** I will have to come back with the number.

**Senator Marwah:** I would like to know what the number is.

**Mr. Boucher:** It is a successful amount.

**Mr. Adam:** I can give you an estimate for the total recruiting efforts of the RCMP but that is not specifically tailored to meet the needs of a small technical contingent that wouldn't necessarily need to go through Depot.

I do have a permanent resource tasked with recruiting for technological purposes across Canada. Like my friend said, what the RCMP does offer the students is in two different ways. On engineering side, instead of working for a big company where they're producing one small aspect of an entire component, our employees are working from the start in the design and conceptual stage right to the deployment of a sharp end tool in the field. That gives them a great deal of gratification as well.

pour des entreprises en démarrage, pour Google ou pour Facebook, malgré les problèmes que ces entreprises ont.

Autrement dit, quel pourcentage de vos budgets serait consacré au recrutement, à la formation et à la recherche vous permettant de rester à l'affût des développements?

**M. Boucher :** Je peux certainement commencer, car le Centre de la sécurité des télécommunications a de l'expérience sur le terrain.

Vous ne devriez pas trouver surprenant que les Canadiens soient motivés par d'autres choses que l'argent. Les entreprises en démarrage et la vie sur la côte Ouest de n'importe quel pays présentent à n'en pas douter des attraits pour les gens, mais la noble cause d'être là à défendre la nation et à veiller à la sécurité des Canadiens réussit aussi à en faire revenir certains.

Au CST, nous perdons parfois d'excellents talents. Je suis fier de dire que souvent, ils nous reviennent parce que l'attrait de travailler pour remplir les poches de quelqu'un d'autre s'étiole rapidement, après avoir eu la voiture sport et le bel appartement, et ils constatent qu'il manque un sens à leur vie. Ils reviennent.

C'est un élément de succès que nous avons maintenant. Je ne vous mentirai pas; c'est un défi constant et nous devons continuer d'offrir un lieu de travail attrayant pour les jeunes, un lieu qui peut s'adapter aux cultures changeantes des jeunes générations, qui peut suivre le rythme de la technologie et qui offre de la formation constante, et ainsi de suite. Je pense que vous comprenez très bien cela. C'est à nous qu'il incombe d'offrir cet environnement. Je suis désolé, mais je n'ai par les chiffres relatifs aux ressources que nous consacrons à ces efforts.

**Le sénateur Marwah :** Est-ce un montant faible, moyen ou élevé? Avez-vous une idée? Serait-ce 5 p. 100 de votre budget, ou 25 p. 100?

**M. Boucher :** Je vais devoir vous revenir avec les chiffres.

**Le sénateur Marwah :** J'aimerais savoir ce que c'est.

**M. Boucher :** C'est un montant qui assure notre succès.

**M. Adam :** Je peux vous donner une estimation du total des efforts de recrutement de la GRC, mais cela ne vise pas la réponse aux besoins particuliers d'un petit contingent technique qui ne passerait pas nécessairement par la Division Dépôt.

J'ai une ressource permanente qui a pour tâche de recruter des gens à des fins technologiques à l'échelle du Canada. Comme mon ami l'a dit, la GRC offre deux choses aux étudiants. Du côté du génie, plutôt que de travailler pour une grande société où ils sont appelés à produire un petit aspect d'une composante complète, nos employés participent au processus entier, de l'étape de la conception à celle du déploiement d'un outil utilisé à l'avant-scène, sur le terrain. C'est très gratifiant pour eux.

The additional thing we have is called handcuffs. Not that we handcuff our people. What we do is we put handcuffs on bad guys. If we can, we attribute the efforts of any single person within the civilian core working for engineers, technicians, cyber-fighters and hackers, et cetera, to an arrest, and we make a big deal about it, because the uniqueness that we offer to any employee is to catch a bad guy. It's very successful in retention of our employees, those who are driven by that.

**Ms. Merchant:** I interact a lot internationally with our allies and so forth, and this is not a unique problem in any way, shape or form. One of the things we're finding is that we need to start influencing the youth at a very young age because the more we are interconnected and the more things are relying on this digital technology — our financial systems are going to a digital monetary basis and we are going to automated vehicles — there are several things that are coming in the future where we will need more people who are savvy in this area.

We are reaching out to private sector companies and non-profits who do make it their mission to incite in very young people and children this interest and love of digital technologies in every way, shape or form. It's not just the technology piece. We need lawyers who are savvy in this and people who understand accounting. Cyber-insurance is mind-boggling. It's not just a technology piece.

**Senator Stewart Olsen:** Why can't you start seconding from different areas? You will be taking up a lot of the responsibilities of different departments, such as FINTRAC. I would think the people who work in FINTRAC would already be half-developed on the investigative aspect.

I would think that as you pull together, the funding should also come from the different departments into this centre. Have you given any thought to perhaps seconding our own people that we have a foot up with? I know it would be a fight but still, I think that would be a very good way to go forward.

**Ms. Merchant:** Well, from my perspective, what I see across the departments is we rely very heavily on secondments and assignments between departments to build the expertise and to better understand how all these moving pieces fit together. It's a critical tool in our tool box.

**The Chair:** I want to thank you all very much. This has been extremely helpful to us and we are very appreciative that you are as focused on this issue as you are, because we've come to learn, as you obviously know, this is a substantial threat not only to government, but to business. We obviously need to protect our country from that kind of threat. Thank you for what you do and thank you for being here today.

L'autre chose, c'est ce que nous appelons les menottes. Pas que nous menottions nos gens. Nous menottons les méchants. Si nous le pouvons, nous soulignons les efforts de tout membre civil de l'effectif qui travaille pour les ingénieurs, les techniciens, les personnes qui luttent contre les pirates informatiques et autres si ces efforts mènent à une arrestation. Nous faisons un effort particulier pour souligner cela, parce que ce que nous offrons d'unique à nos employés, c'est l'occasion d'arrêter un méchant. Cela nous aide grandement à garder nos employés — ceux que cela motive.

**Mme Merchant :** J'entretiens beaucoup de rapports à l'échelle internationale avec nos alliés, entre autres, et cela n'a rien d'un problème unique. L'une des choses que nous constatons, c'est que nous devons commencer à influencer les jeunes très tôt, car plus nous sommes interconnectés et plus nous comptons sur la technologie numérique — nos systèmes financiers se numérisent et nous nous dirigeons vers les véhicules automatisés —, plus nous aurons besoin de gens qui sont habiles dans ce domaine pour tout ce qui s'en vient.

Nous tendons la main aux sociétés du secteur privé et aux organismes sans but lucratif dont la mission est d'insuffler aux jeunes et aux enfants l'intérêt et le goût pour les technologies numériques de toutes les manières possibles. Il n'y a pas que l'aspect technologique. Nous avons besoin d'avocats qui s'y connaissent, et de gens qui comprennent la comptabilité. L'assurance contre les incidents cybernétiques est stupéfiante. Il n'est pas question que de la technologie.

**La sénatrice Stewart Olsen :** Pourquoi ne vous mettez-vous pas à détacher des gens de divers secteurs? Vous allez assumer une grande partie des responsabilités de divers ministères, comme le CANAFE. Je serais portée à croire que les gens qui travaillent au CANAFE seraient déjà à mi-chemin sur le plan de leurs capacités d'enquête.

Je serais portée à croire qu'avec le regroupement, le financement devrait aussi être transféré des divers ministères au centre. Avez-vous pensé à détacher de vos propres gens? Je sais que ce serait difficile, mais je pense quand même que ce serait une excellente façon d'aller de l'avant.

**Mme Merchant :** De mon point de vue, ce que nous voyons dans les ministères, c'est que nous comptons beaucoup sur les détachements et sur les affectations entre ministères afin de favoriser l'acquisition de compétences et la meilleure compréhension de la façon dont toutes les pièces mobiles s'imbriquent. C'est un élément crucial de notre coffre à outils.

**Le président :** Je vous remercie tous beaucoup. Vous nous avez fourni de l'information extrêmement utile et nous vous savons gré d'accorder autant d'attention à cet enjeu, car nous en sommes venus à apprendre, comme vous le savez manifestement, que c'est une menace importante non seulement pour le gouvernement, mais aussi pour le monde des affaires. Nous devons évidemment protéger notre pays contre ce genre de

menaces. Je vous remercie de ce que vous faites, et je vous remercie d'avoir été là aujourd'hui.

(The committee adjourned.)

(La séance est levée.)

## EVIDENCE

OTTAWA, Thursday, March 22, 2018

The Standing Senate Committee on Banking, Trade and Commerce met this day at 11:30 a.m. to study and report on issues and concerns pertaining to cyber security and cyber fraud.

**Senator Douglas Black** (*Chair*) in the chair.

[*English*]

**The Chair:** Good morning and welcome, colleagues and members of the general public who are following today's proceedings on the Standing Senate Committee on Banking, Trade and Commerce. My name is Doug Black. I'm a senator from Alberta, and I chair this committee.

Mr. Carlin, I'm going to ask the senators to introduce themselves so you know who is in the room with us in Ottawa.

**Senator Wetston:** Howard Wetston, Ontario.

**Senator Marshall:** Elizabeth Marshall, Newfoundland and Labrador.

**Senator Unger:** Betty Unger, Alberta.

**Senator Marwah:** Sabi Marwah, Ontario.

**Senator Wallin:** Pamela Wallin, Saskatchewan.

[*Translation*]

**Senator Ringuette:** Pierrette Ringuette from New Brunswick.

[*English*]

**Senator Stewart Olsen:** Carolyn Stewart Olsen, Ontario.

[*Translation*]

**Senator Dagenais:** Jean-Guy Dagenais from Quebec.

[*English*]

**The Chair:** This morning is our eighth meeting on our study on issues and concerns pertaining to cyber security and cyber fraud, including cyber threats to Canada's financial and commercial sectors, the current state of cyber security technologies, and cyber security measures and regulations in Canada and abroad.

## TÉMOIGNAGES

OTTAWA, le jeudi 22 mars 2018

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 11 h 30, afin d'étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude.

**Le sénateur Douglas Black** (*président*) occupe le fauteuil.

[*Traduction*]

**Le président :** Bonjour, chers collègues et membres du public qui suivent aujourd'hui les délibérations du Comité sénatorial permanent des banques et du commerce. Je m'appelle Doug Black. Je suis un sénateur de l'Alberta et président du comité.

Monsieur Carlin, je vais commencer par demander à mes collègues sénateurs de se présenter afin de vous familiariser avec les membres du comité qui prennent part, ici à Ottawa, à la séance d'aujourd'hui.

**Le sénateur Wetston :** Howard Wetston, de l'Ontario.

**La sénatrice Marshall :** Elizabeth Marshall, de Terre-Neuve-et-Labrador.

**La sénatrice Unger :** Betty Unger, de l'Alberta.

**La sénatrice Marwah :** Sabi Marwah, de l'Ontario.

**La sénatrice Wallin :** Pamela Wallin, de la Saskatchewan.

[*Français*]

**La sénatrice Ringuette :** Pierrette Ringuette, du Nouveau-Brunswick.

[*Traduction*]

**La sénatrice Stewart Olsen :** Carolyn Stewart Olsen, de l'Ontario.

[*Français*]

**Le sénateur Dagenais :** Jean-Guy Dagenais, du Québec.

[*Traduction*]

**Le président :** Nous en sommes ce matin à notre huitième séance consacrée à l'étude des questions et préoccupations relatives à la cybersécurité et à la cyberfraude, y compris les cybermenaces posées aux secteurs canadiens du commerce et de la finance, l'état de la technologie en matière de cybersécurité ainsi que les mesures et les règlements adoptés en matière de cybersécurité, tant au Canada que dans d'autres pays.

I am pleased to welcome, from San Francisco, John P. Carlin, Chair, Global Risk and Crisis Management, Morrison & Foerster LLP, which would be one of the leading law firms in the world. We welcome and thank you for joining us, Mr. Carlin. If you would be kind enough to begin with your opening statement and then the senators will have questions.

**John P. Carlin, Chair, Global Risk and Crisis Management, Morrison & Foerster LLP:** Thank you, senator. It's a pleasure to be with you this morning from San Francisco. I can't think of a topic more important to the security of Canada, the United States and the world. It's gratifying to see the interest of this committee on the subject.

I would like to give a brief overview of the threat and some changes that were made in terms of how the United States responds to that threat and then turn it over to questions.

One thing I saw when I was heading the National Security Division, which was the first new litigating division at the United States Department of Justice in about 50 years, it was a division created after the tragedy of September 11 to ensure that, in the future, we effectively shared what we learned on the intelligence side of the house about new and evolving threats over to the law enforcement side of the house so that, as lawyers, we could work creatively based on what the intelligence showed us the threat to be, to come up with ways to disrupt the threat and change the metric of success so that success was no longer holding someone accountable after the terrorist act had occurred when families were grieving or had lost loved ones. That success was seeing where the threat was going and preventing the attack from occurring in the first place.

I give you that background because, when I was there, one area where we saw the threat changing was cyber-enabled attacks. I will give one example. We were watching, both in the United States and Canada, as the Islamic State and the Levant became more sophisticated at using social media, exploiting it, just as al Qaeda had used Western technology — in that case, aviation— to turn it against us and into a weapon, we were watching the Islamic State and the Levant adopt a strategy of crowdsourcing of terrorism. They tried to turn human beings into weapons by reaching out to them from their safe havens abroad and encouraging them to kill where they live.

That caused an immense increase in the number of cases we were handling at the Department of Justice linked to international terrorism.

J'ai le plaisir d'accueillir, de San Francisco, M. John P. Carlin, président, Risques mondiaux et gestion de crise, au cabinet Morrison & Foerster s.r.l., un des grands cabinets d'avocats du monde. Monsieur, soyez le bienvenu. Je vous remercie d'avoir répondu à notre invitation. Auriez-vous l'amabilité de commencer par nous présenter votre exposé, après quoi les membres du comité auraient des questions à vous poser.

**John P. Carlin, président, Risques mondiaux et gestion de crise, Morrison & Foerster s.r.l. :** Merci, monsieur le sénateur. C'est avec plaisir que je me joins à vous ce matin depuis San Francisco. Je ne pense pas qu'il y ait de sujets qui revêtent plus d'importance pour la sécurité du Canada, celle des États-Unis et du monde entier. Je constate avec satisfaction l'intérêt que votre comité porte à la question.

Je voudrais, si vous le voulez bien, commencer par un rapide survol des menaces qui se présentent et de certains des changements que nous avons, aux États-Unis, apportés aux mesures prises en réponse à cette menace. Après cela, c'est très volontiers que je répondrai à vos questions.

Lorsque j'étais chef de la Division de la sécurité nationale, la première nouvelle division contentieuse à être créée au sein du département américain de la Justice en plus de 50 ans. Cette section a été créée à la suite de la tragédie du 11 septembre. Il s'agissait de faire en sorte que les services de renseignement communiquent aux autorités de police et de justice les renseignements qu'ils recueillaient sur les nouveaux risques qui sont apparus, afin que nous, les avocats, puissions trouver de nouveaux moyens de lutter contre les menaces révélées par les services de renseignement, et modifier nos critères de réussite pour qu'il ne soit désormais plus seulement question de punir les actes de terrorisme, mais d'anticiper les menaces et de prévenir les attaques.

Je vous donne un peu de contexte, car une des nouvelles menaces que nous avions cernées à l'époque était celle des attaques qui s'appuient sur des moyens informatiques. Permettez-moi de vous citer un exemple. Tant aux États-Unis qu'au Canada nous observions comment l'État islamique en Irak et au Levant commençait à exploiter habilement les médias sociaux, tout comme Al-Qaïda avait retourné contre nous une technologie occidentale — en l'occurrence l'aviation — en s'en servant comme une arme. Nous voyions, donc, l'État islamique en Irak et au Levant élaborer une stratégie d'externalisation ouverte pour assurer le financement de ses activités terroristes. L'EIIL se proposait de transformer des êtres humains en armes de destruction, les contactant à partir de lieux sûrs où ils étaient hébergés à l'étranger et en les encourageant à perpétrer des attentats dans leur pays de résidence.

Cela entraîna une très forte augmentation du nombre de dossiers de terrorisme international pris en charge par le département de la Justice.

One of those cases shows us, I think, where the cyber threat is going. Imagine a Canadian company with a trusted brand throughout the world that discovers there is a relatively unsophisticated hack, a small amount of personally identifiable information that has been stolen. This is happening to the vast majority of companies throughout the world day in and day out.

In this case, after that information was stolen, and it looked like they had handled the information, they got a note through Gmail with spelling errors that said, essentially, "Hey, we're mad you threw us off your system, and we want you to let us back on to your system, and if you don't we are going to embarrass you by releasing the fact we have gotten into your system and stolen this information. And, by the way, we want about $500 worth of bitcoin."

Again, the vast majority of companies would not view this as a high-risk threat. It looked as if they successfully kept the individual off the system.

What makes cyber different— and I know this committee has been struggling with— is the problem of attribution. If that company had not worked with law enforcement that was fed by the intelligence, including information from our Five Eyes partners, we would never have found it wasn't the criminal it looked like. He was a criminal. It was a guy named Ferizi who had moved from Kosovo to Malaysia, which is from where he launched this attack with a co-conspirator. He was a criminal and he really wanted that $500. But he also had become friends, through Twitter, with one of the most notorious terrorists in the world at the time— a man named Junaid Hussain, who had moved from around London, where he had been convicted, and then released as a computer hacker, had become an extremist, and moved to the very heart of the Islamic State of the Levant in Raqqa, Syria.

He never met Ferizi, the Kosovo extremist who moved to Malaysia, in the real world. They became friends entirely online and through Twitter. What Junaid Hussain convinced Ferizi to do was take this personally identifiable information that was stolen from a trusted retail brand inside the United States and give it to him.

Junaid Hussain was not interested in $500. What he was interested in, consistent with the Islamic State of the Levant, was crowdsourcing of terrorism ideology, and using that information to try to kill. He culled through that list to look for the names of what looked like American law enforcement or state officials and

Une de ces affaires illustre les nouvelles tendances en matière de cybermenace. Imaginez le cas d'une entreprise canadienne dont la marque est favorablement connue dans le monde entier qui s'aperçoit qu'une intrusion informatique d'une envergure relativement réduite a permis de s'approprier une modeste quantité de renseignements personnels. Il s'agit là de quelque chose qui arrive presque tous les jours à la vaste majorité d'entreprises.

Or, en l'occurrence, après le vol des renseignements, l'entreprise, qui a le sentiment d'avoir pris toutes les mesures nécessaires pour sauvegarder son réseau, reçoit, dans un courriel contenant des erreurs d'orthographe le message suivant : « Vous nous avez fortement mécontentés en nous fermant l'accès à votre système, et nous voulons que vous nous permettiez à nouveau d'y accéder. Si vous refusez, nous vous mettrons dans un grave embarras en publiant le fait que nous sommes parvenus à nous introduire dans votre système et à vous voler un certain nombre de renseignements. Nous exigeons en outre que vous nous remettiez 500 $ de bitcoin. »

La grande majorité des entreprises ne se sentiraient pas vraiment menacées par ce genre d'incident. En l'occurrence, l'entreprise avait en effet, réussi à bloquer l'accès à son système.

Mais la différence que fait l'emploi de moyens informatiques — et je sais que votre comité se penche actuellement sur la question — se situe au niveau de l'attribution. Si l'entreprise en question n'avait pas travaillé de concert avec la police et la justice, qui avaient, elles-mêmes, reçu des services de renseignement un certain nombre d'informations, y compris des renseignements transmis par nos partenaires au sein du Groupe des cinq, nous n'aurions jamais réussi à identifier le malfaiteur. Il s'agissait en fait d'un type dénommé Ferizi qui, originaire du Kosovo, était allé vivre en Malaisie d'où, avec l'aide d'un complice, il a lancé son attaque. Ce criminel souhaitait effectivement soutirer 500 $ à l'entreprise en question, mais, par l'intermédiaire de Twitter, il s'était de plus lié d'amitié avec un des terroristes les plus notoires au monde, un certain Junaid Hussain, qui avait quitté les environs de Londres, une fois remis en liberté, après avoir purgé une peine d'emprisonnement pour piratage informatique, s'était radicalisé et était allé s'installer à Raqqa, en Syrie, au cœur même de l'État islamique au Levant.

Il n'a, en fait, jamais rencontré Ferizi, l'extrémiste kosovar qui était allé vivre en Malaisie. Les deux s'étaient liés d'amitié entièrement sur Internet, par le truchement de Twitter. Junaid Hussain a convaincu Ferizi de lui remettre les renseignements personnels qu'il avait volés à la grande marque américaine.

Junaid Hussain n'était pas particulièrement intéressé par les 500 $, mais ce qu'il voulait, conformément à l'idéologie de l'État islamique au Levant, c'était utiliser la stratégie d'externalisation ouverte pour financer une activité terroriste et, en l'occurrence, utiliser les renseignements en question pour

then used the information stolen from the retailer to create a kill list. By using Twitter, they pushed back out to the United States with specific instruction to kill these people by name where they live. They call this threat the "blended threat."

répandre la mort. Il étudia la liste des noms qui lui avait été fournie afin de repérer les personnes qui pourraient appartenir soit à la police, soit à d'autres organismes officiels, son but étant d'établir une liste de personnes auxquelles il pourrait s'attaquer. Par l'intermédiaire de Twitter, il a pu distribuer ces noms aux États-Unis, accompagné d'instructions ordonnant l'assassinat de ces personnes nommément désignées, ses instructions comprenant des indications précises sur leur domicile. On appelle ce type d'action une « menace mixte ».

This is one version of it, where it looks like, and really was for one purpose in the criminal sphere and hitting the private sector, turns into another sphere in the way the information is distributed where it can be used to kill, for terrorism, for another purpose.

Ce cas représente une version de ce type de menace où une activité criminelle visant uniquement le secteur privé se transforme en une autre menace criminelle lorsque la dissémination de renseignements volés peut servir à commettre des meurtres, des actes terroristes ou d'autres crimes.

In this case, the two parties — the government and the private sector— worked very well together, and effective action was taken. Ferizi was arrested pursuant to the United States law enforcement process in Malaysia and ultimately extradited and sentenced to 20 years of incarceration in the state of Virginia.

En l'occurrence, les deux parties intéressées — le gouvernement et le secteur privé ont mené conjointement une action efficace qui a permis de juguler la menace. Ferizi a pu être arrêté en Malaisie en vertu d'un mandat américain, et il a été extradé vers les États-Unis où il a été condamné, en Virginie, à 20 ans de prison.

Junaid Hussain, who is in ungoverned space outside the rule of law in Raqqa, Syria, was killed in a publicly acknowledged military strike by central command.

Junaid Hussain, qui se trouvait à Raqqa, en Syrie, dans un lieu sans gouvernement et hors d'atteinte de la loi, a été tué lors d'une frappe militaire dont la responsabilité a été revendiquée par le commandement central des forces américaines.

In order to deal with this blended threat, as you can see from that case, it's extraordinarily complex. You have to be able to share information across national boundaries. That case alone involved five to six different countries. You need to be able to do it at the speed and scale of the threat, which in cyber moves very quickly. Then you need to have a blended approach. Just like the threat is blended, the approach to response needs to be blended that cuts across different tools of state power. In this case, the military tools were used, state department diplomatic efforts were used in order to do the extradition. The criminal justice system was used, intelligence authorities, including sharing arrangements with Five Eyes partners, were used to try to figure out who did it.

Cet exemple illustre bien l'extraordinaire complexité de ces menaces mixtes. Il faut, d'abord, pouvoir se communiquer les renseignements nécessaires entre divers pays. Cinq ou six pays différents étaient impliqués dans l'exemple que je viens de citer. Dans le cyberespace, tout se passe très vite, et il faut donc pouvoir agir avec la vitesse et l'ampleur de moyens qu'appelle la menace en question. Pour répondre à une menace mixte, il faut une approche qui soit mixte elle aussi, et qui fasse appel à l'éventail complet des moyens dont dispose un État. On a, en l'occurrence, recouru à l'outil militaire, mais ce sont les efforts diplomatiques du département d'État qui ont permis d'obtenir l'extradition. Pour identifier le coupable, il a fallu un effort conjoint de la justice pénale et des services de renseignements ainsi que la coopération de nos partenaires au sein du Groupe des cinq.

As complicated as those intergovernmental moves are of sharing information, what makes this different than the response and the changes prior to September 11, and where we, in the United States, are still figuring out how to make this part of the equation more efficient is, as complicated as the intergovernmental sharing, even more complicated is how do we incentivize private sector companies, who are now, as this case demonstrates, on the front end of national security risks, to share information with speed and scale to government so it can be acted upon?

Ces échanges de renseignements entre gouvernements sont compliqués, mais il convient de noter la différence par rapport à ce qui se faisait avant la tragédie du 11 septembre et les États-Unis s'attachent continuellement à renforcer l'efficacité des moyens mis en œuvre, car, ce qui est encore plus compliqué que la coopération intergouvernementale, c'est comment obtenir la coopération des entreprises du secteur privé, puisque, comme nous venons de le voir, les menaces qui pèsent désormais sur les entreprises privées créent un nouveau problème de sécurité nationale. Il nous faut donc maintenant trouver le moyen de persuader les entreprises de communiquer certains

On the other side of the equation, how do we in government get better at sharing information often collected in the first instance through sensitive sources and methods? For years, the default has been it's classified and stays only within government or shared with close partners like Canada. How do we get better at speed and scale, sharing that information back to the private sector so they know what the threat is?

One area we changed was we started using the criminal justice system in conjunction with the Treasury department's ability to authorize sanctions to make the information public. That started with the first case of its kind in 2014 where we indicted five members of the People's Liberation Army Unit 61398 for economic espionage. It included a case involving an individual who travelled to Canada where we needed law enforcement cooperation with Canada, named Su Bin who ultimately was brought to the United States and charged with economic espionage, to making public using a statement from the FBI on the North Korean attacks on Sony Pictures, to the indictment of members linked to the Iranian Revolutionary Guard Corps for their attacks on the financial sector. We went from never having brought a case linked to national security actors through the criminal justice system, to starting to more regularly bring such cases.

Most recently is the indictment through Mueller's special council investigation of the 13 Russians for their role in undermining confidence in the fair and free democratic elections inside the United States.

The criminal justice system alone can't solve the problem, but we found it's a good vehicle for making public what we are seeing, being able to share with the private sector and partners around the world and use that as a basis to take other actions, be they defensive measures or working with partners on things like sanctions.

Thank you again, and I'm happy to take your questions.

**Senator Stewart Olsen:** Thank you for being with us today. It's actually pretty terrifying what you're talking about.

renseignements au gouvernement, et cela à une échelle et à une vitesse permettant d'intervenir utilement.

Cela dit, il faut que le gouvernement arrive lui-même à améliorer la communication de renseignements obtenus de sources et par des moyens qui doivent demeurer confidentiels. Pendant des années, la pratique habituelle était de classifier ces documents et de ne jamais les communiquer, si ce n'est qu'à des partenaires privilégiés tels que le Canada. Comment accroître la vitesse et l'ampleur des échanges de renseignements afin de tenir le secteur privé au courant des menaces qui se profilent?

C'est ainsi que, par exemple, nous avons allié l'action de la justice pénale à celle du département du Trésor qui a l'autorité nécessaire pour imposer des sanctions, ce qui nous a permis de rendre publics certains renseignements. Un premier exemple de cela remonte à 2014, lorsque nous avons inculpé d'espionnage économique cinq membres de l'Unité 61398 de l'Armée de libération populaire. Il y a également eu l'affaire d'un certain Su Bin qui s'était rendu au Canada, et nous avions donc dû solliciter la coopération des services policiers de votre pays. L'individu en question a été transféré aux États-Unis où il a été inculpé d'espionnage économique. On a aussi rendu publics les renseignements recueillis par le FBI au sujet d'une attaque menée par la Corée du Nord sur la société américaine Sony Pictures, et inculpé des personnes liées au Corps des Gardiens de la révolution islamique qui avaient commis des attaques contre des entreprises du secteur financier. Nous n'avions jamais auparavant intenté de poursuites pénales contre des personnes attentant à la sécurité nationale, mais nous faisons maintenant cela plus régulièrement.

Rappelons la récente inculpation, dans le cadre de l'enquête menée par M. Mueller, le procureur spécial, de 13 ressortissants russes en raison de leur rôle dans des activités portant atteinte à la confiance de la population américaine dans le système électoral des États-Unis.

La justice pénale ne peut pas, à elle seule, résoudre le problème, mais c'est un bon moyen de diffuser auprès du public les faits dont nous avons connaissance, et de communiquer certains renseignements au secteur privé et à nos partenaires dans diverses régions du monde, cela facilitant la prise des mesures qui s'imposent, qu'il s'agisse d'actions défensives, ou d'une action conjointe avec nos partenaires afin de mettre en œuvre un régime de sanctions, par exemple.

Encore une fois, c'est très volontiers que je répondrai à vos questions.

**La sénatrice Stewart Olsen :** Je vous remercie de votre participation à nos délibérations d'aujourd'hui. Vous nous entretenez là d'un sujet assez effrayant.

I notice there seemed to be two components, a reactive and proactive. I know reactive and quick responses is where we absolutely have to work, but proactively, what should we be doing?

**Mr. Carlin:** So I put that in two buckets of potential proactive activity. One that's linked to reactive would be deterrents. Right now, in terms of the capabilities, the ability of those on offence to attack outstrips the technical ability to defend. To phrase it another way, there is no Internet-connected system right now that's safe from a dedicated adversary who wants to penetrate the system. That's true of nation states, North Korea, Iran, Russia or China, but also increasingly true for sophisticated organized criminal groups.

One element of the proactive strategy needs to be defining in advance what red lines are that are going to hopefully engender response that cuts across nation state lines and says we have certain principles such as one should not target a private company with state means, be they military or intel services for the benefit of that private company's competitor. That's the agreement President Obama and President Xi reached after the PLA indictment that then the G20 adopted. That's an example of a clear red line occurring. Another example now would be if you take steps to undermine free and fair democratic elections, there will be a response.

My own view is part of that setting of the red line should include essentially a dead man switch. If we reach the conclusion you meddled with a free and fair election or violated another red line, we won't tell you exactly what the response will be, but in advance we will say there will be a response and we can list the elements of that response to include multilateral sanctions against the behaviour, similar to regimes we have had in other areas like the use of chemical weapons or terrorism. That's bucket one.

Bucket two would be improving defensive practices. Part of that is educating and making clear that if there is no Internet-connected system safe from a dedicated adversary's attack, we need to encourage through regulation and through education the idea of risk management and resilience so there is planning in both the private sector and government as well as to what you do the day after the breach to ensure you can continue to deliver core services and confine the damage.

Il semble y avoir deux aspects à la question, les mesures réactives et les mesures proactives. Je suis consciente du besoin de réagir sans perdre de temps, mais sur le plan proactif, que devrions-nous faire?

**M. Carlin :** Il y a, d'après moi, deux catégories de mesures proactives. L'une d'entre elles entretient d'ailleurs des rapports très étroits avec les mesures réactives. Il s'agit des mesures dissuasives. À l'heure actuelle, sur le plan technique, l'attaquant dispose de moyens beaucoup plus nombreux que le défenseur. Autrement dit, aucun système informatique relié à l'Internet n'est actuellement à l'abri d'un adversaire déterminé qui souhaite s'y introduire. Cela est vrai des États nations tels que la Corée du Nord, l'Iran, la Russie ou la Chine, mais cela devient de plus en plus vrai des organisations criminelles possédant les moyens nécessaires.

Un des fondements d'une stratégie proactive est la définition, par avance, de lignes rouges dont le franchissement déclenchera, espère-t-on, une réaction qui ne s'arrêtera pas à la frontière de l'État. Il s'agit, en effet, de poser certains principes tels que celui interdisant à un État de s'en prendre, par des moyens militaires ou par l'action de services de renseignement, à une entreprise du secteur privé d'un autre État, afin d'avantager un concurrent de l'entreprise en question. Le président Obama et le président Xi s'étaient entendus sur ce point après l'inculpation de certains membres de l'Armée de libération populaire, inculpation qu'avaient par la suite avalisée les pays du G20. Voilà l'exemple d'une ligne rouge à ne pas franchir. Un autre exemple serait l'ingérence dans des élections libres et démocratiques, ce qui entraînerait une réaction de la part du pays attaqué.

D'après moi, la définition d'une ligne rouge devrait s'accompagner de la mise en place d'un dispositif d'homme mort. Cela veut dire que si nous avons des raisons de penser que vous vous êtes immiscé dans une élection libre et juste, ou que vous avez franchi une ligne rouge dans un autre domaine, nous ne vous dirons pas comment nous allons réagir au juste, mais vous devrez savoir que nous allons réagir, y compris par des sanctions multilatérales comme nous l'avons fait dans d'autres domaines tels que le terrorisme ou les armes chimiques. Voilà, donc, une première catégorie de mesures.

Une deuxième catégorie de mesures concerne l'amélioration des pratiques défensives. Il s'agit en partie d'éduquer les secteurs intéressés, et de leur faire comprendre qu'aucun système relié à l'Internet n'est à l'abri d'une attaque de la part d'un adversaire déterminé. Il faut, à la fois, par une réglementation adaptée et un effort de pédagogie, inculquer l'idée de la gestion des risques et du besoin d'assurer la résilience de nos réseaux informatiques. Cela suppose, de la part tant du gouvernement que du secteur privé, un certain effort de planification, mais aussi la mise en place de mesures qui permettront, en cas de pénétration d'un système, de limiter les dégâts et de continuer à assurer les services essentiels.

**Senator Wetston:** Thank you for being with us today. I would like to congratulate you on your exceptional work in the public service in the United States. It is obviously important work, and even becoming more important as you bring that skill set to the private sector, so congratulations.

I would like to pursue two areas with you, if I may. One is in the area of cooperation that you're discussing. I'm not sure if you're aware of this or not, but in the most recent budget of our federal government, they have outlined a national cybersecurity strategy. It was just last week. I won't get into it with you, but I'm sure you would agree with the notion of having a national cybersecurity strategy.

One of the things I wanted to pursue with you is there was a noticeable absence of what I consider to be a very important part of this, which is the role of the Department of Justice. Why do I say that? Obviously our Department of Justice would be very involved with all of the entities that have come before us, but I have not seen any Justice officials appear before us that I recall. I wanted to ask your advice on this given your experience in the U.S. I know you've dealt with Canadians in a great deal.

You were in a position at the National Security Division, which you said was created as a result of 9/11. Would it be your advice, looking at the situation today, that would be a necessary type of activity and role that a Justice department might take and should develop?

I know you've spoken in the past about the risk mitigation associated with the various types of entities we deal with today; crooks, nation states, terrorists. That variety poses special problems. I'm sort of asking an institutional question if you can share that with us.

**Mr. Carlin:** Thank you, sir. I do think it is something to consider.

One of the reasons we did the shift was linked originally to terrorism, which was an area that cuts across both national lines and across the traditional divide between the collection and use of intelligence, on the one hand, and on the other hand, the use of the criminal justice system. I know administering that system, post the reform, at least in the United States, the ability to be able to make use of that intelligence information was vital to confronting the threat in a way that ultimately saved lives. It's almost more important in some respects in this new arena when it comes to the cyberthreat for exactly the reason you outlined,

**Le sénateur Wetston :** Je vous remercie d'avoir accepté de prendre part à nos délibérations d'aujourd'hui. Je tiens à vous féliciter du travail exceptionnel que vous avez accompli dans le cadre des fonctions que vous occupiez au sein de l'administration américaine. C'est une tâche manifestement urgente dont l'importance va d'ailleurs croissante alors que vous êtes appelé à employer vos compétences au sein du secteur privé. Je vous en félicite.

Il y a deux domaines que je souhaiterais aborder avec vous. Le premier concerne la nécessaire collaboration que vous évoquiez tout à l'heure. Peut-être savez-vous que dans son dernier budget, le gouvernement canadien a posé les bases d'une stratégie nationale en matière de cybersécurité. Cela ne date que de la semaine dernière. Je ne souhaite pas aborder avec vous la question de manière détaillée, mais vous êtes sans doute d'accord sur l'idée d'une stratégie nationale en matière de cybersécurité.

Une des questions que je voudrais évoquer avec vous est, par contre, la remarquable absence, dans ce budget, d'un élément extrêmement important. J'entends par cela le rôle du ministère de la Justice. Qu'est-ce qui me porte à évoquer ce sujet? Il est clair que notre ministère de la Justice aurait un rôle important à jouer en liaison avec les divers organismes ayant comparu devant notre comité. Or, je ne me souviens pas que nous ayons entendu des représentants du ministère de la Justice. Compte tenu de l'expérience que vous avez acquise dans ce domaine aux États-Unis, j'aimerais obtenir sur ce point votre avis. Je sais que vous avez beaucoup travaillé avec des fonctionnaires canadiens.

Vous avez exercé des fonctions au sein de la Division de la sécurité nationale, service qui, vous l'avez dit, a été créé en réponse aux attentats du 11 septembre. Étant donné la situation actuelle, y a-t-il effectivement, selon vous, une activité et un rôle qui reviendraient en cela au ministère de la Justice?

Vous avez, par le passé, évoqué les efforts d'atténuation des risques liés aux diverses catégories d'acteurs : les criminels, les États-nations et les terroristes. Cette dernière catégorie pose d'ailleurs des problèmes particuliers. Je vous demande donc de nous donner votre avis sur la répartition des rôles entre les divers organes de l'État.

**M. Carlin :** C'est en effet, monsieur le sénateur, une question qui mérite d'être posée.

Si nous avons modifié notre dispositif, c'était à l'origine à cause du terrorisme, phénomène qui fait fi des frontières nationales et qui, de plus, ignore la division traditionnelle des tâches entre, d'une part, la collecte du renseignement et l'usage qui en est fait, et d'autre part l'action des organes de justice pénale. Je sais qu'aux États-Unis, les changements qui ont été apportés au fonctionnement des divers services de l'État, et la possibilité, désormais, d'avoir accès aux informations recueillies par les services de renseignement ont joué un rôle essentiel dans la défense contre les nouveaux risques qui se présentent, et cela

the multiplicity of threat actors— criminal, crooks, spies/nation states. The Ferizi case is just one example of this increasing trend of blended threat.

I'll use Russia as one example. We've seen case after case now where there's a huge cybercrime problem. One estimate according to one nonprofit, CSIS, says approximately $650 billion last year alone in global theft. That, however, is not totally amorphous. Behind that threat is one country in part, Russia.

They are doing another study now but some estimates would say nearly 50 per cent of that crime is emanating from Russian-organized criminal groups who do not respond to requests for law enforcement cooperation to hold those groups responsible.

Recently there was a case where the criminal group was literally called Infraud and its motto was "In fraud we trust." It was a group where criminals got together and combined tools they had to hack into companies, used stolen information from one place to sell to another. They had reviews that would say whether or not it was a trustworthy crook, just like Amazon. It would say, "Five stars. I've bought from this crook before. His information is fantastic."

Or, which always amuses me: "Two stars. This crook is not trustworthy. I don't recommend buying from them."

So that's on the one hand, the criminal side. On the other side we're seeing links with the intelligence service of Russia. There was the Yahoo breach where, according to the indictment that's been made public, when the United States asked for law enforcement cooperation against one of the top 10 thieves of credit card information in the world, instead of providing cooperation, the Russian intelligence services signed that individual up as a source and started making use of the information he was stealing.

So when you see how blended that threat is, it becomes difficult, I think, for a criminal justice system to respond effectively unless it can make use of— and has the legal right to make use of — some of the information collected on the intelligence side of the house. And vice versa. It's very hard to have an effective response nationally and with partners unless you can talk publicly about what you're seeing.

nous a permis d'éviter des morts. Or, à certains égards et pour des raisons dont vous nous avez fait part, en l'occurrence la multiplicité des auteurs de menaces, dont des criminels, des malfaiteurs, des espions et des États-nations, cela revêt une importance encore plus grande sur le plan des cybermenaces. L'affaire Ferizi n'est qu'un exemple de ce phénomène croissant de la menace mixte.

Je vais maintenant prendre l'exemple de la Russie. De multiples affaires démontrent l'ampleur du problème de la cybercriminalité. Selon le Center for Strategic and International Studies, le vol a, à l'échelle mondiale, rapporté l'année dernière environ 650 milliards de dollars. Or, il ne s'agit pas d'un phénomène entièrement amorphe. En effet, la menace provient en partie d'un pays bien précis, en l'occurrence la Russie.

Une autre étude est en cours à ce sujet, mais d'après certains calculs, presque 50 p. 100 de ce type de criminalité émane d'organisations criminelles russes. Or, la Russie ne donne pas suite aux demandes qui lui sont adressées par des organisations policières qui souhaiteraient obtenir sa coopération afin de poursuivre les responsables de ces organisations criminelles.

On a récemment eu connaissance d'une organisation criminelle qui avait pris pour nom le mot Infraud, et qui s'était donné pour devise « In fraud we trust ». Il s'agissait de criminels qui s'étaient regroupés, mettant en commun leurs moyens et leurs connaissances afin de pirater les systèmes informatiques de certaines entreprises, et revendre les renseignements qu'ils parvenaient à voler. Comme Amazon, ils avaient un système de classement indiquant, par exemple, « Cinq étoiles. J'ai déjà acheté des informations à ce malfaiteur, c'est un fournisseur digne de confiance ».

J'en ai aussi vu une qui m'a beaucoup amusé : « Deux étoiles. On ne peut pas faire confiance à ce brigand. Je ne peux pas le recommander comme fournisseur. »

Voilà, donc, pour l'aspect criminel du phénomène. Mais on constate en outre l'existence de liens entre le volet criminel et les services de renseignements russes. Après le piratage des systèmes de Yahoo, certains individus ont été publiquement inculpés, mais lorsque les États-Unis ont demandé aux autorités russes de coopérer dans le cadre de poursuites intentées contre un des dix principaux voleurs de données de carte de crédit au monde, au lieu de collaborer, le renseignement russe s'est attaché les services de l'individu en cause et ont entrepris de se servir des données qu'il arrivait à subtiliser.

Ainsi, s'agissant de menaces mixtes, la justice pénale ne peut pas agir efficacement si on ne lui reconnaît pas le droit, et qu'on ne lui donne pas les moyens de se servir de certaines informations recueillies par les services de renseignement. L'inverse est également vrai. Il est extrêmement difficile d'intervenir de manière efficace, tant sur le plan national qu'au niveau de l'action menée avec des partenaires étatiques, si l'on

The criminal justice system is a great tool to make public so one can have the conversation and then work together to say, "How do we raise the costs to our adversaries so they stop this behaviour," on the one hand, and to the prior senator's question, "How do we make clear what we're seeing tactically so that private sector companies can invest proactively in how to defend themselves?"

**Senator Wetston:** Thank you very much.

**Senator Wallin:** Thank you. I appreciate your comments so far today. Most interesting.

We just were hearing testimony yesterday from our own government officials on their state of readiness and putting together systems and coordination between departments, et cetera.

Two comments on related issues. First, how many countries do you believe have dead man's switch capability now, that could actually react and are reacting without, as you say, making a lot of public noise?

Secondly, I was just reading a piece this morning in the wake of all of the Facebook stuff. You talked earlier about weaponizing people. It was interesting. We have Julian Assange, who is considered, of course, a villain in the piece, and Mark Zuckerberg has always been wonder boy and man of the year. But essentially both of them have either knowingly or unknowingly weaponized data and people.

I would just like your thoughts on that. Thank you.

**Mr. Carlin:** On the first, right now I don't think there is a mature deterrence system in cyber that is consistently applied across countries. It's a place we need to get to. There has been an increase, which is a positive trend.

If you think of the approach as three prongs— we used to keep it secret. When it comes to cyber, we are actually much better at attribution than the average public would think, and the reason they didn't think we were any good at it is because we kept it all secret for a while.

One, we need to figure out who did it. Two, make it public more often as a matter of course. And three, after making it public, impose consequences.

ne peut pas faire état publiquement des activités dont on prend connaissance.

Or, la justice pénale facilite le débat public et favorise la coopération. Il s'agit en effet de travailler ensemble afin de faire pression sur nos adversaires pour qu'ils changent de comportement. Et j'ajoute, en réponse à la question posée par le sénateur qui est intervenu un peu plus tôt, qu'il s'agit de faire prendre conscience aux entreprises du secteur privé, de la situation que nous constatons sur le terrain afin de les encourager à investir dans des moyens de défense proactifs.

**Le sénateur Wetston :** Merci.

**La sénatrice Wallin :** Je vous remercie. Je prends un vif intérêt à ce que vous venez de nous dire.

Nous avons recueilli, hier, le témoignage de représentants de nos services officiels qui ont évoqué le niveau de préparation, les systèmes actuellement mis en œuvre, et les mesures de coordination instaurées entre les divers ministères.

J'aurais deux questions à vous poser sur des sujets connexes. En premier lieu, d'après vous, combien de pays ont actuellement instauré un dispositif d'homme mort qui permettrait, effectivement, de prendre des contre-mesures sans ébruiter la chose?

Deuxièmement, j'ai lu ce matin un article sur les retombées de l'affaire Facebook. Vous avez parlé plus tôt de l'arsenalisation des personnes. C'est une question du plus grand intérêt. D'un côté, il y a Julian Assange, qui, dans la pièce, occupe le rôle du méchant, et puis il y a Mark Zuckerberg, le jeune prodige. Mais en fait, consciemment ou inconsciemment, les deux ont arsenalisé à la fois des données et des personnes.

Pourriez-vous nous donner votre avis à ce sujet. Je vous remercie.

**M. Carlin :** Je dois dire, sur le premier point, que nous ne disposons pas actuellement, dans le cyberespace, de moyens de dissuasion adaptés à la menace et susceptibles d'être employés à l'échelle transnationale. Or, nous allons devoir y parvenir. Des progrès encourageants ont cependant été faits dans ce sens.

Imaginez une approche à trois piliers. À une certaine époque, tout cela restait secret. Or, s'agissant de cybermenaces, nos résultats en matière d'identification des coupables sont bien meilleurs que le public ne pourrait le penser et, si les gens n'avaient pas à l'époque une grande confiance en nos capacités, c'est parce que notre action est pendant longtemps demeurée secrète.

Donc, dans un premier temps, il nous faut parvenir à identifier le coupable. Et puis, il nous faut, plus généralement, publier le nom des responsables et, dans un troisième temps, les sanctionner.

Recently you have see attribution to the North Koreans of the ransomworm WannaCry— which did an enormous amount of indiscriminate damage— and subsequently NotPetya, the Russian-related version of the ransomware started in the Ukraine that caused nearly $1 billion worth of damage— again, indiscriminately — throughout the world as it went and locked up different systems ranging from hospitals to corporations.

You've seen actions now of publicly doing the attribution to say WannaCry was North Korea and NotPetya was Russian. It was a little slow, but it's better that it was done.

What you have not seen afterwards in terms of your deterrence retribution point, you haven't seen, really, effective collective action on the scale of what occurred. I'm concerned if we don't act collectively by going public without effective action we're actually sending the opposite message and encouraging more and more irresponsible and provocative behaviour through cyber means.

On your second issue, the issue of weaponizing information, it's something we've learned and are starting to adjust to but still working on. When you look at, for instance, what happened with the North Korean attack on Sony, I can tell you we "war gamed" for years what it would look like if a rogue nuclear armed state attacked the United States through cyber means and we never figured it was going to be about a movie about a bunch of pot smokers, that this was going to be the big national security incident or first of its kind.

One thing you learned about that case is it was a destructive attack. It turned computers, essentially, into bricks. Number two, it involved large-scale theft of intellectual property. Both threats we thought a lot about before.

It's not really why anyone remembers that the attack, though. What they remember about the North Korean attack on Sony was the weaponizing of information, the theft of salacious emails from inside the company that were used by untraditional media to distribute and then mainstream media picked up on those and became, essentially, part of the North Korean plan to try to stop Sony from exercising free speech.

That's a very difficult— first we need to identify that that's the new tactic. We saw something similar that the Russians then did in the elections. It's a harder problem to stop, but I think you're right; it starts with awareness of how it occurs. Then the next step, I think, is for those who are masters of that technology in the private sphere to start addressing their resources to see

Comme vous avez pu le voir récemment, on a réussi à imputer aux Nord-Coréens le rançongiciel Wannacry — qui a causé, aveuglément, d'énormes dégâts. Puis, il y a eu NotPetya, un ver informatique rançonneur que l'on doit à des groupes russes, et qui, à partir de l'Ukraine, a fait, à travers le monde et sans la moindre discrimination, presque 1 milliard de dollars de dégâts en bloquant tout un éventail de systèmes, aussi bien dans des hôpitaux que dans des entreprises commerciales.

Or, vous avez constaté que, désormais, nous n'hésitons pas à attribuer, disons, Wannacry à la Corée du Nord, ou NotPetya aux Russes. Nous avons un peu tardé à le faire, mais il est, d'après nous, préférable de dénoncer publiquement les responsables.

Ce qui manque, cependant, au niveau de la dissuasion, c'est une action collective efficace proportionnée à l'attaque. Ce qui m'inquiète, c'est que si nous dénonçons publiquement les responsables, sans engager en même temps une action collective efficace, nous faisons passer le mauvais message et, en fait, nous encourageons les actes irresponsables et provocateurs de cybercriminels.

Quant au second point que vous avez soulevé, l'arsenalisation des informations, c'est un phénomène relativement nouveau que nous commençons à affronter. Prenons l'exemple de l'attaque nord-coréenne contre la compagnie Sony. Je suis en mesure de vous dire que pendant des années, nous avons mené des exercices de simulation afin de voir un peu comment un État dévoyé possédant un arsenal nucléaire s'y prendrait pour lancer une cyberattaque contre les États-Unis. Eh bien, nous n'avions jamais imaginé qu'une telle attaque serait déclenchée à l'occasion d'un film sur les aventures d'un petit groupe de fumeurs de pot, que cela allait prendre une telle importance sur le plan de la sécurité nationale et constituer, en quelque sorte, une véritable première.

Or, cette attaque a fait de gros dégâts. Elle a essentiellement neutralisé des systèmes informatiques. Et puis, elle a permis le vol d'une vaste quantité de propriété intellectuelle. Nous avions, avant cela, longuement réfléchi à ces deux types de menaces.

Ce n'est cependant pas pour cela qu'on se souviendra longtemps de ces attaques. Ce qu'il faut retenir, en effet, de l'attaque menée par les Nord-Coréens sur Sony, c'est qu'on a assisté à l'arsenalisation des renseignements volés. Des courriels graveleux internes à la compagnie ont été repris par des médias non traditionnels, puis par la presse généraliste, tout cela faisant partie du plan ourdi par les Nord-Coréens et visant à bâillonner Sony.

Tout cela soulève de grandes difficultés, car il faut en premier lieu percer la nouveauté des tactiques employées. Lors des élections, les Russes ont mis en œuvre des moyens analogues. C'est un problème très compliqué, mais je pense que vous avez raison, il faut d'abord comprendre comment ils s'y prennent. Après cela, il faut que les acteurs du secteur privé qui maîtrisent ces diverses technologies mobilisent leurs moyens afin de voir

how they can stop their platforms from being abused to weaponize information.

**Senator Wallin:** Just a quick follow-up. Other than Mr. Zuckerberg's apology and "Gosh, we're going to look into this," I mean, this is a big issue. What can and should he do in the next 15 minutes or few days?

**Mr. Carlin:** Making it broader than one company, because there are a variety of different social media companies now and with the new technology has come new ways, creative ways, to exploit it by the terrorist groups or nation states.

Earlier on the big issue we were confronting, when I was on the criminal side, with the first social media was those who exploit children started using the platforms and you saw the companies get more and more sophisticated at applying new technology that would identify child pornography content, got better at coming up with non-profit, non-governmental groups that stored that information. Any company could tap their expertise to use it, such as NCMEC, the National Center for Missing and Exploited Children. That combined effort helped to thwart that issue.

We applied a similar model when it came to terrorist exploitation of social media that has really improved the response of social media companies now from where they were three or four years ago.

What you're raising is this use by nation states to put fake news or other means to influence elections. That's the newer threat. I think the resources, expertise and changes we saw when it came to child exploitation and terrorism are a good model.

What makes this version particularly hard— and I don't pretend this one is easy— is how it conflicts with our first amendment in the United States but in Canada the general recognition of a right of speech and how do you administer the system in a way that's consistent with that fundamental democratic and civil society virtue while confronting this threat.

There, I think it's figuring out ways to confront an anonymity and have transparency as to who the speaker is. That is, admittedly, easier said than done.

**Senator Unger:** Thank you very much, Mr. Carlin, for your presentation.

You talked a lot about cooperation being a very essential component of trying to deal with these threats. How does Canada compare in terms of, I guess, cooperation but, also, our own

s'il ne serait pas possible d'empêcher que leurs plateformes servent à arsenaliser l'information.

**La sénatrice Wallin :** Je vais vous demander, très rapidement, une petite précision. Nous avons vu que M. Zuckerberg s'est excusé, ajoutant qu'il allait naturellement se pencher sur le problème. Mais, la situation est grave. Quelle mesure devrait-il prendre dans l'immédiat?

**M. Carlin :** Il faut élargir le problème à toutes les entreprises de médias sociaux, car les nouvelles technologies mises en œuvre offrent aux groupes terroristes et à certains pays de nouveaux moyens d'exploiter la situation.

À l'époque où je participais à l'action répressive, le gros problème se situait au niveau des premiers médias sociaux, dont certains individus se servaient pour diffuser de la pornographie infantile. Or, les entreprises ont appris à employer de nouvelles technologies pour repérer ce type de contenu, et des organismes non gouvernementaux à but non lucratif ont entrepris l'archivage des données permettant de repérer les responsables. Les entreprises pouvaient ainsi faire appel aux connaissances d'organismes tels que le National Center for Missing and Exploited Children. La mise en commun des efforts a permis de brider la dissémination de ce genre de contenu.

C'est par ces mêmes moyens que les entreprises de médias sociaux ont considérablement amélioré leurs capacités de freiner l'exploitation de leurs plateformes par des terroristes. La situation à cet égard s'est sensiblement améliorée ces trois ou quatre dernières années.

Vous soulevez là le problème des fausses nouvelles diffusées par certains pays pour peser sur les élections. C'est une menace d'un type nouveau, mais je pense que les ressources, les connaissances et les mesures qui ont servi à freiner l'exploitation des enfants pourront utilement servir dans ce nouveau contexte.

Ce qui aggrave en l'occurrence les difficultés — car je ne prétends pas que cela sera facile — c'est l'antinomie entre les moyens qui vont devoir être employés et l'exercice des droits découlant, aux États-Unis, du premier amendement de la Constitution. Le Canada garantit, lui aussi, la liberté d'expression et il s'agit donc d'instaurer un système qui tout en contrecarrant les menaces qui se présentent respecte cette liberté fondamentale d'une société démocratique.

Il faut ainsi trouver le moyen de percer le voile de l'anonymat et de faire la lumière sur les auteurs d'actes contre lesquels nous devons nous défendre. Je reconnais que cela n'est pas facile.

**La sénatrice Unger :** Je tiens à vous remercier, monsieur Carlin, de l'exposé que vous nous avez présenté.

Vous avez insisté sur la nécessaire coopération, un élément tout à fait essentiel des efforts visant à contrer ces menaces. Que pourriez-vous nous dire de ce que fait actuellement le Canada sur

readiness and any weaknesses that you would care to comment on?

**Mr. Carlin:** I wouldn't presume to judge the Canadian expertise, because I'm more an expert on U.S. law and government.

One suggestion that the senator had raised before as an area to look at, and that I know we have been moving towards and has been helpful, is what your mechanism is for taking what's collected from the national security and intelligence side of the house and turning that into product, whether it's by using the criminal justice system or other means that can help feed both critical infrastructure but also the public at large as to what the threat is and what defensive measures they can take to effectively confront that threat.

That's an area where more work, I think, needs to be done. A second issue would be to continue to improve mechanisms for speedy cooperation across borders so that law enforcement action can be taken in one country on behalf of the other, while being respectful of that country's laws and institutions. Right now, the cyber adversaries shoot the gap and they'll commit activity in one country that affects many other countries.

The more we can move towards speed-of-cyber information sharing, and then the ability to apply that information regardless of where the individual lives, the better.

**Senator Unger:** You created a threat analysis team to study potential national security challenges posed by the Internet of Things. Would you explain that, please?

**Mr. Carlin:** I'm glad you asked. If you think conceptually, one reason we're here studying this issue is that, over a 25- to 30-year period, we moved almost everything we value in the West from analogue form — books and papers — to digital form, and then connected it through an Internet protocol — TCP-IP — that was never designed for security. We did so without properly calculating the risk from making that move as terrorists, crooks, spies and nation states moved to exploit this now digitally stored information that's connected through the Internet.

That's where we are now, playing a game of catch-up in terms of laws, regulations and practices of both the private and public sectors. The Internet of Things would be an exponential increase in the surface area of devices that are online digitally, sharing information and connected through that same insecure protocol,

le plan de la coopération? Où nous situons-nous au niveau des préparatifs, et quelles seraient, selon vous, les faiblesses de notre dispositif?

**M. Carlin :** Vous savez, mes connaissances concernent essentiellement le droit américain et l'action du gouvernement des États-Unis, et je ne saurais me prononcer sur les actions menées en ce domaine par le gouvernement canadien.

Le sénateur a mentionné précédemment une chose à envisager, ce vers quoi je sais que nous nous dirigeons, et que cela a été utile, c'est-à-dire le mécanisme par lequel prendre ce qui a été recueilli par le côté sécurité nationale et le côté renseignement et transformer cela en produit, que ce soit par le truchement du système de justice pénale ou d'autres moyens qui pourraient informer non seulement l'infrastructure critique, mais aussi le public en général quant à la nature de la menace et aux mesures défensives qu'il pourrait prendre pour s'en protéger.

C'est un domaine dans lequel, à mon avis, il y a encore beaucoup de travail à faire. Un deuxième enjeu serait de continuer à améliorer les mécanismes de coopération transfrontalière rapide de sorte que les forces d'application de la loi dans un pays puissent prendre des mesures au nom de l'autre pays, tout en en respectant les lois et institutions. À l'heure actuelle, les cyberadversaires profitent de l'écart et commettent dans un pays une activité qui se répercutera dans de nombreux autres pays.

Plus vite nous avançons vers un partage de renseignements à la vitesse du cyberespace, plus grande sera la capacité d'appliquer ces renseignements indépendamment de là où une personne vit.

**La sénatrice Unger :** Vous avez créé une équipe d'analyse des menaces chargée d'étudier les menaces éventuelles à la sécurité nationale que représente l'Internet des objets. Pouvez-vous expliquer cela?

**M. Carlin :** Je suis heureux que vous me le demandiez. Sur le plan conceptuel, une des raisons pour lesquelles nous sommes ici à étudier cette question, c'est que sur une période de 25 à 30 ans, nous avons transféré presque tout ce qui est précieux pour nous dans l'Ouest de l'analogue — livres et documents — au numérique, puis nous avons relié tout ça par un protocole Internet — TCP/IP — qui n'avait jamais été conçu en fonction de la sécurité. Nous avons fait cela sans calculer correctement le risque d'une telle démarche si des terroristes, des escrocs, des espions et des États-nations exploitaient ces renseignements maintenant stockés sous forme numérique et reliés par Internet.

Et voilà où nous en sommes maintenant, à courir pour rattraper la situation sur le plan des lois, des règlements et des pratiques tant dans le secteur public que dans le secteur privé. L'Internet des objets représenterait une augmentation exponentielle du nombre de dispositifs en ligne, partageant des renseignements et

the Internet. That ranges from your refrigerator, to your lights, to the cars on the road.

If you think about it, what we shouldn't do is make the same mistake we did when it was just data that we were moving. These are real objects, and if you look in the United States, we have already had a proof of concept hack that showed through the entertainment system, one could access the core braking and steering systems of a car that caused a recall of 1.4 million Jeep models that had already been sold to the United States public.

We also had a proof of concept hack with pace makers, medical devices that were actually in people's bodies — in their hearts — where a 12-year-old could essentially hack and kill. When they originally rolled out, they were well tested and they worked, but what they didn't do is test whether they would work if someone deliberately tried to make them not work as designed.

This is a critical moment for our respective governments to not make the same mistake again of not thinking through risk and try to ensure and incentivize that there is security by design so before the device is rolled out and reaches the general public, it's as secure as it can be against this type of threat.

That can range from, instead of having default unencrypted devices, having the default be that they're encrypted and password protected, to when it comes to something like an automobile, ensuring the entertainment system and core braking and steering systems are segregated by design so a bad guy who gets into one can't jump over to the other.

The reason we had the group studying it is it's such an important moment to get this right before we've already moved and made ourselves vulnerable and people's lives are actually lost, at which point I'm sure we will have the incentive and drive to fix it. But let's fix it before someone is either hurt or dies.

**Senator Marshall:** Thank you very much. As Senator Wetston said, our federal budget came down last month, and there's a very small, obscure section in the budget that proposes the sharing of confidential tax information on Canadian taxpayers with other countries around the world. Based on the information I had, it would probably be 20 or 30 countries and would include the U.S., China and Russia, as well as a number of other countries.

Do you have any knowledge of what the U.S. is doing with regard to the sharing of tax information with other countries? What do you see as the risks associated with the sharing of confidential tax information with other countries?

reliés par ce même protocole non sécurisé, l'Internet. Cela va du réfrigérateur à l'éclairage, aux voitures sur la route.

À bien y penser, nous ne devrions pas commettre la même erreur que quand il ne s'agissait que de données à déplacer. Ici, ce sont des objets réels, et aux États-Unis, nous avons déjà eu une preuve de possibilité de piratage dans le cas duquel l'accès est passé par le système de divertissement d'une voiture, entraînant le rappel de 1,4 million de modèles Jeep qui avaient déjà été vendus au public américain.

Nous avons vu aussi une preuve de possibilité de piratage de stimulateurs cardiaques, des dispositifs médicaux qui se trouvaient de fait dans le corps de personnes — dans leur cœur — qu'un enfant de 12 ans serait capable de pirater et de détruire. Quand ces dispositifs ont commencé à être installés, ils avaient été très bien testés et ils fonctionnaient parfaitement, mais ce que les essais n'ont pas fait, c'est de déterminer s'ils fonctionneraient correctement si une personne tentait délibérément de les empêcher de fonctionner comme prévu.

Le moment est crucial pour nos gouvernements respectifs de ne pas commettre la même erreur en ne déterminant pas les risques potentiels et ne tentant pas de faire en sorte que la conception tienne compte de la sécurité avant que le dispositif ne soit mis en service et atteigne le public, qu'il soit aussi sécurisé que possible contre ce type de menace.

Pour faire cela, par exemple, au lieu d'avoir des dispositifs non cryptés par défaut, il faudrait les avoir cryptés par défaut et protégés par mot de passe, et quand il s'agit d'une chose comme une automobile, s'assurer que le système de divertissement et les systèmes essentiels de freinage et de direction soient, de par leur conception, entièrement séparés de sorte qu'un malfaiteur qui arrive à accéder à l'un ne puisse sauter dans l'autre.

Nous avons constitué le groupe d'étude sur cette question parce qu'il est extrêmement important de faire correctement les choses avant que nous devenions vulnérables et que des gens perdent la vie. À ce stade, je suis sûr que nous serons pleinement motivés à régler le problème, mais réglons-le avant que quelqu'un ne soit blessé ou n'en meure.

**La sénatrice Marshall :** Merci beaucoup. Comme l'a dit le sénateur Wetston, notre budget fédéral a été présenté le mois dernier, et il s'y trouve une toute petite section, obscure, qui propose le partage des renseignements fiscaux confidentiels sur les contribuables canadiens avec d'autres pays. D'après les renseignements que j'ai reçus, ce serait probablement 20 à 30 pays, dont notamment les États-Unis, la Chine et la Russie.

Êtes-vous au courant de ce que les États-Unis font en ce qui concerne le partage des renseignements fiscaux avec d'autres pays? Quels sont d'après vous les risques associés à un tel partage des renseignements fiscaux confidentiels?

**Mr. Carlin:** I'm really not an expert on the sharing of confidential tax information. I know to access it, for U.S. law enforcement purposes, there is a special regime and authority called the 26 U.S.C. 6103 that governs when you can use it for investigating potential crimes, but I don't know the rules and procedures for sharing it at the request of a partner.

I've seen some requests that came in through multilateral assistance treaty requests, but I apologize, senator, I'm not aware of the provision.

Generally, it's a type of information I know we invested resources in to try to improve the security around the theft of that information through cyber-enabled means. It was one of the areas of focus when we learned the hard way through the OPM, the Office of Personnel Management, breach where we lost so much information about government employees.

Across the board, in government, we did something called a cybersprint to improve the basic blocking and tackling, if you will, of cybersecurity and start identifying crown jewel information that needs to be protected, and that tax information would fall into the category of sensitive information that needs extra protections.

I also know, on the other hand, sharing that information to track down criminals, terrorists, nation states and tax evaders is important, and so is having secure means with authorities to share.

**Senator Marshall:** You talked about the blending of information, so that people who are interested in gaining confidential information can get it from this source and they match it up with other information and combine it to use it for other illicit purposes. Do you see that as a possibility?

**Mr. Carlin:** Sure. If you went on the so-called Dark Web today, that portion of the Internet that's not indexed, and you have to know particularly where you're going, where you see criminals essentially creating bazaars of trade in illicit information. That sensitive information about individuals is for sale and gets a premium, essentially, the more sensitive it is. You're seeing, along with health, general credit information and tax information would be of value.

What you don't know, when it reaches that secondary criminal market, is who is going to obtain it. We've seen nation states use that method to obtain information we worry about. We haven't seen it on scale, the terrorist groups doing the same thing. And

**M. Carlin :** Je ne suis vraiment pas un expert sur le partage des renseignements fiscaux confidentiels. Je sais comment y accéder — à des fins d'application de la loi des États-Unis, il y a une autorité et un régime spécial appelé le 26 U.S.C. 6103 qui régit l'usage de ces renseignements dans les enquêtes de crimes potentiels —, mais je ne connais pas les règles et procédures applicables au partage de ces renseignements à la demande d'un partenaire.

J'ai vu passer certaines demandes qui nous ont été adressées dans le cadre d'un traité d'entraide multilatérale, mais je suis désolé madame, je ne connais pas une telle disposition.

En général, c'est le genre de renseignements pour lesquels je sais que nous avons investi des ressources pour tenter d'en améliorer la sécurité et la protection contre le vol par le truchement de cybermoyens. C'était un des domaines sur lequel on s'est penché lors de la catastrophe du Bureau de la gestion du personnel des États-Unis quand nous avons perdu tant de renseignements au sujet d'employés du gouvernement.

À l'échelle du gouvernement entier, nous avons procédé à ce qu'on appelle un sprint cybernétique pour améliorer les mesures fondamentales de blocage et d'attaque, si vous voulez, pour la cybersécurité, et nous avons commencé à repérer les renseignements les plus cruciaux qui doivent être protégés; les renseignements fiscaux se trouvent dans cette catégorie de renseignements délicats qui nécessitent une protection supplémentaire.

Je sais aussi, d'autre part, que le partage des renseignements pour trouver des criminels, des terroristes, des États-nations et des fraudeurs de l'impôt est important, et donc il est aussi important de disposer de moyens sécurisés par lesquels les autorités peuvent échanger des renseignements.

**La sénatrice Marshall :** Vous avez parlé du mélange de renseignements, de sorte que les personnes qui aimeraient obtenir des renseignements confidentiels pourraient les obtenir de cette source, puis les comparer à d'autres renseignements et les combiner pour les utiliser à des fins illicites. Est-ce une possibilité d'après vous?

**M. Carlin :** Bien sûr. Si l'on va sur le Web invisible aujourd'hui, cette portion d'Internet n'est pas indexée, et il faut savoir exactement où on va, où des criminels tiennent essentiellement des bazars d'échange de renseignements illicites. Ces renseignements personnels délicats sont en vente et obtiennent un prix d'autant plus élevé s'ils sont délicats. Comme vous pourrez le constater, avec les renseignements sur la santé, les renseignements généraux de crédit et fiscaux seraient de grande valeur.

Une fois que ces renseignements atteignent le marché criminel secondaire, on ne sait pas qui va les obtenir. Nous avons vu des États-nations utiliser cette méthode pour obtenir des renseignements qui nous inquiètent. Nous n'avons pas vu cela à

regularly criminals are selling to each other for different criminal purposes.

**Senator Marwah:** Thank you, Mr. Carlin, for coming and presenting to us today.

You mentioned in several articles you have been interviewed on that in the world of cyber our data rules and regulations are stuck in the 19th century. If we had to go at certain rules and regulations, and one is the data rules surrounding data storage outside the country and now you talked about the Internet of Things, what other regulations need to be addressed?

I suspect your knowledge would probably apply to the U.S., though I suspect that if you have it in the U.S., we will have it in Canada. I appreciate that it might be the same in the U.S. So which ones would you go after?

**Mr. Carlin:** That is a great question. A couple of different areas. One, in the United States now, and we'll see what happens because it's attached to the current budget bill where there is a vote taking place as we talk, but the so-called CLOUD Act, which would be a means by which— one of the problems is let us say there is a Canadian law enforcement matter of a crime of local jurisdiction and a murder takes place in Canada. State and local police are constantly confronting the issue that information critical to that purely local crime of citizen on citizen is often now held by a foreign company overseas. So there is a great frustration from state and local law enforcement that it's not practical for us to routinely use the Mutual Legal Assistance Treaty or MLAT request for these traditional local crimes. That request can take from a year to 18 months to process. They want to be able to use the laws of Canada, to serve process in Canada and get a response for a local crime.

The CLOUD Act would present a mechanism that says, essentially, if the two regimes have equivalent privacy and civil liberty protections, one can use those equivalent legal processes, court orders, to obtain information for local crimes. It sets up a way for two court systems to be able to do that.

On the one hand, I think that's a great model because it encourages countries to raise the bar in terms of the protection of civil rights and civil liberties to get access to that ability to serve process; on the other hand, it modernizes a system that increasingly relies on digital data so you can perform routine law enforcement functions.

grande échelle, mais les groupes de terroristes font la même chose. Et les criminels ordinaires se vendent les uns aux autres des renseignements à différentes fins criminelles.

**Le sénateur Marwah :** Merci, monsieur Carlin, de nous parler aujourd'hui.

Dans de nombreux articles pour lesquels vous avez été interviewé, vous avez mentionné que dans le monde cybernétique, nos règlements sur les données stagnent au XIX[e] siècle. Si nous devions nous attaquer à un certain nombre de règlements, dont celui qui régit le stockage des données hors du pays, et vous parlez maintenant de l'Internet des objets, quels autres règlements devraient être modernisés?

Vos connaissances s'appliquent probablement aux États-Unis, quoique je soupçonne que si vous l'avez aux États-Unis, nous l'avons au Canada. Je pense bien que ce serait la même chose aux États-Unis. Par conséquent, quels seraient ceux auxquels vous vous attaqueriez?

**M. Carlin :** C'est une excellente question. Il y a deux ou trois domaines différents. Premièrement, aux États-Unis, à l'heure actuelle — et nous verrons ce qui va se produire parce que c'est relié à la loi budgétaire pour laquelle un vote se tient en ce moment —, il y a ce qu'on appelle le CLOUD Act, la loi sur le nuage, qui serait un moyen par lequel... Voici le problème : disons qu'il y a une question d'application des lois canadiennes pour un crime de compétence locale et qu'un meurtre est commis au Canada. Les services policiers locaux et d'État sont constamment confrontés au fait que des renseignements cruciaux pour ce crime purement local de citoyen sur citoyen sont souvent en possession d'une société étrangère outre-mer. Par conséquent, c'est une grande frustration pour les agences locales et d'État d'application de la loi qu'il ne soit pas pratique pour nous de recourir de façon routinière à une demande au titre du Traité d'entraide juridique, ou TEJ, pour ces crimes locaux routiniers. Une telle demande peut prendre d'un an à 18 mois avant d'être traitée. Ils veulent pouvoir utiliser les lois du Canada pour signifier des actes au Canada et obtenir une réponse concernant un crime local.

Selon la loi sur le nuage, il y aurait un mécanisme selon lequel, si les deux régimes ont des protections de la vie privée et des libertés civiles équivalentes, un peut utiliser ces actes juridiques et ordonnances équivalents pour obtenir des renseignements concernant des crimes locaux. Ainsi, deux systèmes judiciaires pourraient faire cela.

Par ailleurs, je crois que ce serait un excellent modèle, parce qu'il encourage les pays à lever la barre en termes de protection des droits civils et des libertés civiles en ce qui concerne l'accès à cette capacité de signifier des actes; d'un autre côté, cela modernise un système qui s'appuie de plus en plus sur des données numériques pour l'exécution de fonctions routinières d'application de la loi.

If we don't come up with solutions like that, the worry will be the continued trend towards mandatory data localization, which is not good for civil rights and civil liberties. Also, it's not good for our economic growth development and productivity. Similarly, it is not good for national security purposes, where you want to be able to share information across like-minded information.

So that's one area: modernize our ability to serve law enforcement process consistent with our respective values to obtain information across borders.

Another area would be consistency on data breach notification and requirements. I see this even more now that I'm in the private sector advising clients. It is a dizzying array of different rules and regulations. In the United States alone, we have around 48 different State data breach notification laws, many of which are slightly different. For many companies they're doing business in multiple countries and regions throughout the world simultaneously. A breach usually affects those multiple countries.

So to work together to try to have data breach notification that's consistent or to explore safe harbour ideas where if the bulk of the breach occurs in one country and you meet that country's laws, the other country accepts that as a mechanism for doing breach notification.

Ultimately, what we want to do is incentivize companies to come forward voluntarily with the information.

The third area we've talked about a bit already today would be thinking through the information governments collect and what the mechanisms are to share that with the private sector so they can take action. That's a new problem with this technology. We've never had the private sector so much on the front lines of what used to be core governmental responsibilities and threats like national security threats. We need to rethink our rules and regulations accordingly.

**Senator Marwah:** What about our privacy laws? Do you believe our privacy laws have kept pace with where technology has gone?

**Mr. Carlin:** I think privacy law needs to be iterative. The technology is shifting so quickly that in some areas there has been a lot of focus and attention on personal identifiable information and how to make a notification if that is taken.

Si nous ne produisons pas des solutions comme celle-ci, la tendance actuelle vers la localisation obligatoire des données deviendra inquiétante, parce qu'elle n'est pas bonne pour les droits civils et les libertés civiles. Elle n'est pas bonne non plus pour notre croissance économique et notre productivité. Elle n'est pas bonne encore pour la sécurité nationale, domaine où des entités aux vues similaires devraient pouvoir partager des renseignements entre elles.

C'est donc un domaine : moderniser notre capacité de signifier des actes d'application de la loi qui correspondent à nos valeurs respectives pour obtenir des renseignements transfrontières.

Un autre domaine serait la cohérence des notifications d'atteinte à la protection des données. Je vois encore plus cela maintenant que je suis dans le secteur privé, conseillant des clients. Il y a une gamme étourdissante de règlements différents. Aux États-Unis seulement, nous avons environ 48 lois d'État sur la notification de l'atteinte à la protection des données, dont plusieurs sont légèrement différentes. Dans le cas de nombreuses entreprises, celles-ci font affaire simultanément dans de nombreux pays et de plusieurs régions du monde. Une atteinte à la protection des données touche généralement ces nombreux pays.

Par conséquent, pour collaborer et tenter d'avoir des notifications d'atteinte à la protection des données qui soient cohérentes ou explorer des possibilités de sphère de sécurité quand le gros de la brèche se produit dans un pays et on répond aux lois de ce pays, l'autre pays accepte cela comme mécanisme de notification de l'atteinte à la protection des données.

En fin de compte, nous cherchons à motiver les entreprises à produire volontairement les renseignements.

Le troisième domaine dont nous avons parlé un peu déjà aujourd'hui serait celui des renseignements que les gouvernements recueillent et des mécanismes selon lesquels ces renseignements pourraient être communiqués au secteur privé pour qu'il puisse agir. C'est un nouveau problème avec cette technologie. Nous n'avons jamais eu le secteur privé autant en première ligne de ce qui relevait auparavant de responsabilités fondamentales du gouvernement et des risques comme les menaces à la sécurité nationale. Il nous faut repenser nos règlements en conséquence.

**Le sénateur Marwah :** Et qu'en est-il des lois sur la protection de la vie privée? Estimez-vous que nos lois sur la protection de la vie privée ont suivi l'évolution de la technologie?

**M. Carlin :** Je crois que les lois sur la protection de la vie privée doivent être itératives. La technologie avance si rapidement que, dans certains domaines, il y a eu beaucoup d'attention sur les renseignements personnels identifiables et sur la façon de procéder à une notification si ceux-ci ont été volés.

But the threat to privacy may not be through a breach of that information. It might be the ability to put it together and apply new tools like machine learning or as we develop artificial intelligence to create great opportunities, so you want, on the one hand, incentivize that investment, but also new threats to privacy.

Our respective regimes, they're just at the beginning of thinking through what the implications are of the application of artificial intelligence to bulk data sets and what the rules should be in that area. The technology is changing so quickly. It's new. So that's an area of continued study and hopefully will be a common approach in the future.

[*Translation*]

**Senator Dagenais:** Following the events that took place recently on the Facebook platform, I would like to know whether people can take concrete, individual actions to better protect their identity.

Last year, in an interview on American television, you said that a social insurance number is the primary identifier in both the United States and Canada, but that this method is now outdated. What could replace the social insurance number as a personal identifier, and have actions already been taken or planned, say, by governments, including the American government? I would like to hear your point of view on this issue.

[*English*]

**Mr. Carlin:** I'm glad you raised that issue.

In its first instance, the old social security cards used to say on the card, "Don't use this for identification purposes." Over time, partly encouraged by well-meaning regulation, particularly in the financial sector, we started to require companies use it for exactly that purpose. If that was ever a good idea, it is not now.

The current top official in the Trump administration for cybersecurity, Rob Joyce, has stated publicly that, like many, his personal identifiable information has been stolen at least six times. And it's not particularly helpful as a consumer to get a notice that your information has been stolen, such as your social security number, because what as a consumer can you do with that information?

Mais la menace à la vie privée peut ne pas être par l'atteinte à la sécurité de ces renseignements. Elle pourrait se situer dans la capacité de réunir des renseignements et d'appliquer de nouveaux outils comme l'apprentissage machine, ou encore au fur et à mesure de l'avancement de l'intelligence artificielle pour créer de grandes possibilités, de sorte qu'il y a d'une part une motivation à cet investissement, mais aussi, d'autre part, des menaces à la vie privée.

Nos régimes respectifs en sont tout juste au début de la réflexion sur les conséquences de l'application de l'intelligence artificielle aux ensembles massifs de données et sur ce que les règles devraient être dans ce domaine. La technologie change si rapidement. C'est du nouveau. C'est donc un domaine qui mérite d'être étudié continuellement et, avec un peu d'espoir, il y aura une approche commune à l'avenir.

[*Français*]

**Le sénateur Dagenais :** À la suite des événements qui ont eu lieu récemment sur la plateforme Facebook, j'aimerais savoir si les gens peuvent poser des actions concrètes, individuellement, pour mieux protéger leur identité.

L'an dernier, lors d'une entrevue à la télévision américaine, vous avez dit que le numéro d'assurance sociale est la base de l'identité aux États-Unis tout comme au Canada, mais que cette méthode est maintenant dépassée. Qu'est-ce qui pourrait remplacer le numéro d'assurance sociale pour s'identifier et y a-t-il déjà des actions qui ont été menées ou qui sont en voie de l'être, entre autres par les gouvernements, dont le gouvernement américain? J'aimerais entendre votre point de vue à ce sujet.

[*Traduction*]

**M. Carlin :** Je suis heureux que vous ayez soulevé la question.

Au tout début, l'ancienne carte de sécurité sociale portait la mention « À ne pas utiliser à des fins d'identification ». Au fil du temps, encouragés partiellement par des règlements bien intentionnés, surtout dans le secteur financier, nous avons commencé à exiger que les entreprises l'utilisent exactement à cette fin. Si c'était une bonne idée à l'époque, elle ne l'est plus maintenant.

Le plus haut fonctionnaire actuel dans l'administration Trump pour la cybersécurité, Rob Joyce, a déclaré publiquement que, comme tant d'autres, ses renseignements personnels d'identité ont été volés au moins six fois. Ce n'est pas particulièrement utile pour un consommateur d'être avisé que ses renseignements, comme son numéro de sécurité sociale, ont été volés, parce qu'en tant que consommateur, que peut-il faire de ce renseignement?

I think there is a study group that Rob Joyce has alluded to inside the United States to start examining what it might look like to move from the social security number to other forms of multi-factor identification. It's an area where technology has caused the problem, in part, because so much of what identifies us is stored online and has been stolen, accumulated and is now sold criminally.

But the technology may also be the solution insofar as, going back to the machine learning type part, it may be we have unique identifiers that will identify you in the aggregate by examining many different facets of what you're doing and where you're communicating online. There are multi-factor forms of identification.

It seems like we need to start moving in that direction and quickly. When you look at some of the largest data breaches that have already occurred, let alone how much without a breach at all— things people are making available about themselves online — if we don't move to fix this, it's a problem that's going to cause an increasing amount of loss due to fraud and other means.

[*Translation*]

**Senator Dagenais:** When the perpetrator of a cyberattack is identified, can you tell us how you proceed with charges? Have there been trials in the United States? If so, I would like to know what kind of evidence must be submitted to get convictions.

[*English*]

**Mr. Carlin:** In each instance we followed our normal protocol before bringing a criminal case, even when we thought it was unlikely that we'd be able to obtain the defendant, meaning we had enough evidence that would be admissible in a criminal court, and we believed it more likely than not that a jury of the defendant's peers would convict them beyond a reasonable doubt. And we have brought trials and had people confront evidence in the courts and been successful with those theories.

Often, actually, once seeing the evidence that's admissible against them, many of the defendants have pled guilty when they've been able to reach the U.S. court system, including the one that we couldn't have done without the cooperation from Canada— and I know Canada had been under great pressure at the time from China, and we greatly appreciated the cooperation and the use of the normal procedures of the Canadian criminal justice system in the case I referenced earlier of Su Bin.

Je crois bien que Rob Joyce ait fait allusion à un groupe d'étude aux États-Unis qui commencera à étudier la possibilité de passer du numéro de sécurité sociale à d'autres formes d'identification à facteurs multiples. C'est un domaine où la technologie a causé le problème, en partie, parce qu'un si grand nombre de données qui nous identifient sont stockées en ligne et ont été volées, accumulées, et maintenant vendues à des fins criminelles.

Mais la technologie peut aussi être la solution dans la mesure où, si on revient à l'aspect de l'apprentissage machine, il se pourrait que nous ayons des identificateurs uniques qui nous identifieraient de façon globale en examinant de nombreux aspects différents de ce que nous faisons et des endroits avec lesquels nous communiquons en ligne. Il y a de nombreuses formes d'identification à facteurs multiples.

Il semble que nous devrions commencer à avancer dans ce sens, et rapidement. Si l'on tient compte de certaines des plus grandes brèches qui se sont déjà produites, sans compter toutes les atteintes à la protection des données sans brèche — les choses que les gens révèlent sur eux-mêmes en ligne —, si nous n'agissons pas rapidement pour corriger ce problème, il causera des pertes de plus en plus importantes en raison de fraudes et d'autres moyens.

[*Français*]

**Le sénateur Dagenais :** Lorsque l'auteur d'une cyberattaque est identifié, pouvez-vous nous dire de quelle façon vous fonctionnez en ce qui concerne les mises en accusation? Y a-t-il eu des procès aux États-Unis? Si oui, j'aimerais savoir quel genre de preuves doivent être présentées pour aboutir à des condamnations.

[*Traduction*]

**M. Carlin :** Dans chaque cas, nous avons suivi notre protocole normal avant d'intenter une action au criminel, même quand nous pensions qu'il était peu probable que nous puissions mettre la main sur l'accusé; autrement dit, nous avions suffisamment de preuves qui seraient recevables devant une cour pénale, et nous estimions probable qu'un jury composé de pairs du défendeur trouverait celui-ci coupable hors de tout doute raisonnable. Nous avons intenté des actions en justice, avons confronté des gens à des preuves devant le tribunal et nous avons réussi de cette façon.

Souvent, de fait, une fois confrontés à des preuves contre eux qui sont recevables, plusieurs accusés ont plaidé coupables quand ils avaient accès au système pénal des États-Unis, y compris celui que nous n'aurions pas pu confronter sans la coopération du Canada — je sais que le Canada avait été soumis à d'immenses pressions de la Chine à ce moment-là, et nous sommes reconnaissants de la coopération et du recours aux procédures normales du système de justice pénale canadien dans le cas de Su Bin dont j'ai parlé plus tôt.

In order to do it means having court processes that you can obtain logging in real time, often information using appropriate court processes, where you can essentially examine the bits and bytes and be able to introduce them. What happens often, if it's in the national security sphere, that information may also be collected through intelligence means. That is very hard to introduce in court, so instead try to collect information using normal criminal processes, on the one hand.

The second change that we made was it is bits and bytes and it is electronic evidence, but at the end of the day, it's human beings behind the keyboard. We shouldn't discard the normal investigative techniques that we use, including flipping and gaining the cooperation of witnesses through plea bargains, using undercover agents to penetrate some of these organized criminal groups, and then third, applying techniques like the use of the behavioural analyst unit, the so-called profilers, who for years helped when I used to prosecute serial homicide or sex offence cases. You would get FBI expertise who knew how to examine the forensic evidence and use it to say this is or isn't consistent with a particular behavioural profile.

More recently, the FBI has been having people who are cross-trained as cyber experts and then trained in using the forensic evidence you get in cyber to build a profile of whom the adversary might be. That was a technique we used when trying to figure out who did the Sony attack.

**Senator Ringuette:** Thank you so much for being with us today. I'm going to ask a few simple questions in regard to the example you gave us at the beginning of your comments about corporate awareness and how corporations are cooperating with police authorities.

For instance, I'm amazed a major U.S. corporation, having a blackmail email to get 500 bitcoins, had the awareness to alert your policing authorities. The corporations are kind of in a bind, "Give us 500 bitcoins and your information will not be distributed worldwide," taking into consideration the impact with the customer and the value of the corporation notifying of the breach.

I guess two things: Statistically, how often would such a situation occur? How often would a corporation alert your policing authorities? Should there be regulations in regard to the corporation alerting the police, notifying the police authorities of every little blackmail issue they encounter?

Pour faire cela, il faut avoir des processus judiciaires accessibles par entrée en communication en temps réel, souvent des renseignements obtenus au moyen de processus judiciaires appropriés, lorsqu'il est possible d'examiner les bits et les octets pour pouvoir les présenter. Souvent, lorsqu'il s'agit de la sphère de sécurité nationale, l'information peut aussi être recueillie par le truchement du renseignement, ce qui est très difficile à présenter devant un tribunal; par conséquent, nous tentons de recueillir les renseignements par le truchement des processus de justice pénale ordinaires. C'est une des choses.

Nous avons fait un deuxième changement. Les bits et les octets et les preuves électroniques, c'est très beau, mais en fin de compte, ce sont des êtres humains qui manipulent le clavier. Nous ne devrions pas ignorer les techniques d'enquête normales que nous utilisons, y compris encourager les gens à se retourner contre d'autres et obtenir la coopération de témoins par la négociation de plaidoyers, utiliser des agents d'infiltration pour pénétrer dans certains groupes de crime organisé, puis appliquer des techniques comme le recours aux services d'analyse comportementale, des profileurs, qui, pendant des années, m'ont aidé quand je travaillais à la poursuite d'affaires de meurtre en série et d'agression sexuelle. Nous avions recours aux services experts du FBI qui savaient comment examiner les preuves médico-légales et les utiliser pour déterminer si une chose concordait avec un profil comportemental particulier.

Plus récemment, le FBI a des personnes qui ont suivi une formation polyvalente de cyberexperts, puis ont été formées à l'emploi des éléments de preuve obtenus dans le cyberespace pour bâtir un profil de l'adversaire éventuel. C'était la technique que nous avons utilisée quand nous tentions de déterminer qui avait procédé à l'attaque Sony.

**La sénatrice Ringuette :** Merci beaucoup d'être avec nous aujourd'hui. Je vais vous poser quelques simples questions concernant l'exemple que vous nous avez donné au début de vos remarques au sujet de la conscientisation des entreprises et de la façon dont celles-ci coopèrent avec les autorités policières.

Par exemple, je suis émerveillée de voir qu'une grande entreprise des États-Unis, ayant reçu un courriel de chantage réclamant une rançon de 500 bitcoins, a eu la sagesse d'alerter vos autorités policières. Les entreprises sont un peu entre le marteau et l'enclume; elles sont sommées de payer 500 bitcoins pour que leurs renseignements ne soient pas diffusés à l'échelle du monde, et elles doivent tenir compte de l'impact sur le client et de la valeur de l'entreprise si elles doivent signaler la brèche.

Statistiquement parlant, à quelle fréquence une telle situation se présente-t-elle? À quelle fréquence une entreprise alerterait-elle vos autorités policières? Devrait-il y avoir des règlements concernant la notification de la police par l'entreprise, la notification des autorités policières pour tout petit chantage auquel elles sont confrontées?

**Mr. Carlin:** Statistically it's difficult to answer because — and this has been part of the problem in coming up with the full scope and scale of criminal activity in this space, because we're only aware of the ones that are reported. We've tried to do surveys. I think we did one recently. Some have placed it about a third of companies having received ransomware. Some have placed the number higher based on anonymous surveys.

I know when I was in government— and I see it now in the private sector— it seems like an enormous number of companies, small, mid-sized and large, are being hit on a weekly basis with ransomware type requests. The increase of these extortion ransomware attacks will continue as long as there are a decent number of companies paying off those who are extorting them from overseas. Right now, from the perspective of the crooks, it's a ripe market.

What they usually do is hit in smaller amounts, and that way it's easier to pay than try to report. And in fairness, from the point of view of the company or private sector, I think they think many times what's the point of going to law enforcement with a $300 or $500 ransomware, even a couple of thousand dollars? They're not going to do anything. It's overseas and it just increases the potential nuisance of trying to be responsive or the embarrassment on top of having to do the payment without providing us something helpful in return.

It's a difficult issue, like kidnapping, where there may be circumstances— it's easy to say in the abstract, and the general policy from the FBI is to discourage people from paying ransomware, in part because you're not guaranteed to get the data back anyway, because it increases the likelihood someone else is going to get hit or, if someone finds out that you're a company that's willing to pay, that you'll get hit again.

At the same time, right now, if you don't have the focus on resilience, it could literally be a life-or-death situation in some circumstances. We've seen hospitals and local police departments hit with these requests. For a company, they have to weigh potential loss of life or injury, or a situation that is so material to their ability to do business it would put them out of business, so their fiduciary responsibility versus the payment.

I think it's an area to explore. I'll use the phrase "carrots and sticks," but what are the incentives that would encourage a company to come forward and tell the police? Right now it's a mixed message, at least in the U.S.— and I think it's similar in Canada— where some regulators may use the fact that you came forward against you and to say you had insufficient defences.

**M. Carlin :** Statistiquement c'est difficile à dire, et c'est une partie du problème dans l'établissement de la portée et de l'ampleur complètes de l'activité criminelle dans cet espace, parce que nous ne sommes au courant que de ce dont on est avisés. Nous avons essayé de faire des sondages. Je crois que nous en avons fait un récemment. D'aucuns parlent d'un tiers des entreprises qui ont reçu une demande de rançon par rançongiciel. D'autres parlent d'un nombre beaucoup plus élevé d'après des sondages anonymes.

Je sais que, quand j'étais au gouvernement — et je le vois aussi maintenant dans le secteur privé —, c'était apparemment un nombre très élevé d'entreprises, petites, moyennes et grandes, qui étaient frappées de ce type de demandes de rançon toutes les semaines. L'augmentation de ces attaques d'extorsion par rançongiciels continuera tant qu'il y a un nombre décent d'entreprises qui payent ces rançons à des extorqueurs d'outre-mer. À l'heure actuelle, du point de vue des escrocs, le marché est juteux.

En général, ils demandent de petits montants que l'entreprise trouve plus faciles à payer qu'à signaler. Et, en toute justice, du point de vue de l'entreprise ou du secteur privé, la question est de savoir souvent quel est l'intérêt de s'adresser aux autorités policières pour une demande de rançon de 300 $ ou de 500 $, et même d'un ou deux milliers de dollars? Elles ne vont rien faire. Ça vient d'outre-mer et cela ne fait qu'augmenter le potentiel de dérangement que de tenter de réagir ou de s'exposer à l'embarras, en plus de faire le paiement, sans fournir quelque chose d'utile en échange.

C'est un problème difficile, comme les enlèvements, où il pourrait y avoir des circonstances… c'est facile de dire dans l'abstrait, et c'est la politique générale du FBI que de décourager les gens de payer une rançon, en partie parce qu'il n'y a aucune garantie de récupérer les données de toute manière, parce que cela augmente la probabilité pour quelqu'un d'autre d'être frappé ou, si les escrocs constatent qu'il s'agit d'une entreprise disposée à payer, que celle-ci sera frappée à nouveau.

Parallèlement, à l'heure actuelle, si l'on ne met pas l'accent sur la résilience, ce pourrait littéralement être une situation de vie ou de mort dans certaines circonstances. Des hôpitaux et des services policiers locaux ont été frappés de telles demandes. Pour une entreprise, celle-ci doit peser le pour et le contre de blessures ou pertes de vie éventuelles, ou une situation qui est si essentielle à sa capacité de faire affaire qu'elle ferait faillite; par conséquent, c'est peser la responsabilité fiduciaire contre le paiement.

Je crois que c'est un domaine à explorer. J'utiliserai l'expression « la carotte et le bâton », mais quels incitatifs encourageraient une entreprise à se manifester et à prévenir la police? À l'heure actuelle, le message est ambigu, au moins aux États-Unis — et je crois que c'est la même chose au Canada —, où certaines autorités de réglementation pourraient utiliser contre

Others are encouraging you to come forward as a victim. It's a bit of a mixed message.

I think we should review the carrots and sticks and decide, as a policy matter, if we want companies coming forward routinely, they should get something in return for coming forward, even if that means some immunity from liability. You have to find the right balance so that you do it in a way that doesn't encourage people to have lax procedures. You need to have procedures that encourage resilience and preparation so if they get hit with ransomware, they don't need to pay and they can get back to doing business.

**Senator Tkachuk:** Just a couple of questions. On the question of cybersecurity, there's the criminal element of people trying to steal stuff, but there's also, as Senator Marwah talked about, the question of privacy. You mentioned the Internet of Things and fridges all being tied into the Internet and all the rest of it.

I'm wondering about the invasion of your own home by cybercrime, people being able to see into your home. We use wireless to access Netflix. I'm always amazed that actually works. We use wireless to access YouTube. Obviously, televisions are becoming much more sophisticated than they used to be, rather than cable. When I use Netflix, if I watch a duster on TV, the next time it comes on it's got a whole bunch of other westerns. So they know what I'm doing. If I watch a show on cable, they don't know what I'm watching unless they phone me and they say, "Are you watching CTV News?" I think they have to phone me; I'm not sure.

How long will it be before wireless can access your home? We have computers in cars. We're talking about self-driving cars. All of those personal things controlled by the Internet, I think they are an even greater threat to our way of life, actually. I wonder if you can comment on any of that nonsense I'm trying to espouse here, but I think it's serious.

**Mr. Carlin:** I think you're right that privacy and cybersecurity are inextricably linked ideas. It's already occurring. Devices are generating more and more telemetric data — information about how the devices are working. There's an enormous upside. We have focused a lot in the cybersecurity hearing, and rightly so, on the down, but that information could save lives when it comes to preventing accidents in the future, or provide critical information to doctors that helps save lives in the health provision.

l'entreprise le fait qu'elle se soit manifestée et déclarer que ses mécanismes de défense sont insuffisants. D'autres sont encouragées à se présenter comme victime. Le message est plutôt ambigu.

Je crois qu'il y aurait lieu de revoir le principe de la carotte et du bâton et, en tant que politique, si nous voulons que les entreprises se déclarent systématiquement, il faudrait leur donner quelque chose en échange pour s'être signalées, même si cela signifie une certaine immunité en matière de responsabilité. Il faut trouver le bon équilibre de sorte que les choses se fassent d'une façon qui n'encourage pas les gens à avoir des procédures laxistes. Il faut qu'il y ait des procédures qui encouragent la résilience et la préparation de sorte que si elles sont frappées d'une demande de rançon par rançongiciel, elles n'aient pas besoin de payer et elles pourraient poursuivre leurs activités normalement.

**Le sénateur Tkachuk :** Je n'ai qu'une ou deux questions. En ce qui concerne la cybersécurité, il y a l'aspect criminel des gens qui tentent de voler des choses, mais il y a aussi, comme l'a dit le sénateur Marwah, la question du respect de la vie privée. Vous avez parlé de l'Internet des objets et des frigidaires qui sont tous reliés sur Internet.

Je m'interroge sur l'invasion de nos logis par le cybercrime, des gens qui sont capables de voir dans notre maison. Nous utilisons le réseau sans fil pour accéder à Netflix. Je suis toujours émerveillé que cela fonctionne vraiment. Nous accédons à YouTube par le réseau sans fil. De toute évidence, les télévisions deviennent plus sophistiquées qu'auparavant avec le câble. Quand je regarde un western sur Netflix à la télé, la fois suivante toute une gamme d'autres westerns m'est proposée. Ils savent donc ce que je fais. Si je regarde un programme à la télé sur câble, personne ne sait ce que je regarde sauf si on m'appelle et me demande si je regarde les nouvelles à Radio-Canada. Je crois qu'il faut qu'on m'appelle par téléphone; je ne suis pas sûr.

Dans combien de temps le réseau sans fil pourra-t-il accéder à nos logis? Nous avons des ordinateurs dans les voitures. On parle de voitures sans conducteur. Je crois que tous ces objets contrôlés par Internet constituent une plus grande menace encore à notre mode de vie. Pouvez-vous commenter certains de ces non-sens que je tente d'exposer ici, qui sont sérieux à mon avis.

**M. Carlin :** Vous avez raison de dire que la vie privée et la cybersécurité sont des idées inextricablement liées. Cela se produit déjà. Des dispositifs génèrent de plus en plus de données télémétriques — des renseignements sur la façon dont les dispositifs fonctionnent. Il y a un énorme avantage. Nous nous sommes concentrés beaucoup à l'audience sur la cybersécurité, et à juste titre, sur les inconvénients, mais ces renseignements pourraient sauver des vies quand il s'agit de prévenir des accidents à l'avenir ou fournir aux médecins des renseignements critiques qui permettront de sauver des vies dans la prestation de soins de santé.

What's key is thinking around the area of, again, security by design. How can we incentivize and encourage rolling out the devices to make sure bad people are not going to use them for unintended purposes? There's work to be done there. In certain regulated industries it's a little ahead, but by and large that's not happening and the devices are rolling out on scale without thinking about the security equation.

Second, we're in a race a little bit. There are countries who don't share our values, who are trying to win the race for artificial intelligence. Whoever wins the race will have a huge advantage in terms of committing future cyber-enabled crime or national security activity. It's going to fuel the way those intrusions and defences work. And then later, the breakthroughs in quantum mathematics might render irrelevant much of what we do to defend right now on the encryption side. So there's a race, too, to see who does quantum first.

In order to win that race, I think you need to incentivize the private sector to be able to collect and analyze that data efficiently. However, the rules and regulations, to your point, should be on use. As we think through it, we should encourage the ability to apply and learn how to analyze that data for productive purposes but set limits on use. That's an area that is newly being explored with the change in technology.

What I'm finding now in the private sector is a lot of companies are starting to collect. That's just the way the device is working. They've never been in this sphere or sector before. They've never thought of themselves as a tech company or information-collecting company, and they're just starting to discuss in the boardrooms and C-Suites, "What does this mean, and what do we do with this data we're collecting?"

So it's a good time for bodies like yours to help set the rules of the road for them as they think about what to do in the future.

**The Chair:** Thank you very much, Mr. Carlin. You have been extraordinarily helpful to us. Your experience, both in the public service and in the private, has been a very helpful combination, and we're indebted to you. Thank you very much for helping us, and you have been a real help.

With that, we will adjourn the hearing, with our thanks to Mr. Carlin in San Francisco. Thank you very much.

(The committee adjourned.)

L'élément clé ici, c'est, une fois de plus, la sécurité au stade de la conception. Comment pouvons-nous motiver et encourager le déploiement des dispositifs d'une façon qui fasse en sorte que des malfaiteurs ne puissent pas les utiliser à des fins non voulues? Il y a du travail à faire sur ce plan. Certaines industries réglementées ont un peu d'avance, mais dans l'ensemble, cela ne se produit pas et les dispositifs sont déployés à grande échelle sans aucune pensée accordée à la sécurité.

Deuxièmement, nous sommes un peu dans une course. Des pays qui ne partagent pas nos valeurs tentent de gagner la course à l'intelligence artificielle. Quiconque gagne cette course aura un énorme avantage pour la commission de crimes ou d'activités contre la sécurité nationale facilitée par le cyberespace. Cela continuera à alimenter les façons dont ces intrusions et les défenses fonctionnent. Ensuite, plus tard, les percées en mathématiques quantiques pourraient anéantir la plupart de ce que nous faisons présentement du côté du cryptage. C'est donc aussi une course au premier qui atteint le quantique.

Pour gagner cette course, à mon avis, il faut motiver le secteur privé à pouvoir recueillir et analyser ces données efficacement. Cependant, les règlements, comme vous dites, devraient porter sur l'usage. Dans notre réflexion à cet égard, nous devrions encourager la capacité d'appliquer et d'apprendre comment analyser les données à des fins productives, tout en limitant l'usage. C'est un domaine nouvellement à l'étude au gré de l'évolution de la technologie.

Dans le secteur privé, je découvre maintenant qu'un grand nombre d'entreprises commencent à recueillir des données. C'est tout simplement la façon dont le dispositif fonctionne. Elles n'ont jamais agi dans cette sphère ou dans ce secteur auparavant. Elles ne se sont jamais vues comme des entreprises de technologie ou des entreprises de collecte de renseignements, et elles commencent tout juste à se demander dans les salles de réunion : « Qu'est-ce que cela signifie-t-il et que faisons-nous de ces données que nous recueillons? »

Le moment est donc propice pour des organes comme le vôtre d'aider à établir pour elles les règles tandis qu'elles réfléchissent à ce qu'elles feront à l'avenir.

**Le président :** Merci beaucoup, monsieur Carlin. Vous nous avez apporté une aide extraordinaire. Votre expérience, tant à la fonction publique que dans le secteur privé, a été une combinaison très utile, et nous vous sommes très reconnaissants. Merci beaucoup de nous avoir tant aidés.

Sur ce, nous levons la séance, avec nos remerciements à M. Carlin à San Francisco. Merci beaucoup.

(La séance est levée.)

WITNESSES

**Wednesday, March 21, 2018**

*Cybersecurity and Privacy Institute, University of Waterloo:*

Florian Kerschbaum, Interim Director.

*Public Safety Canada:*

Colleen Merchant, Director General, National Cyber Security Directorate.

*Royal Canadian Mounted Police:*

Chief Superintendent Jeff Adam, Acting Assistant Commissioner, Technical Operations.

*Communications Security Establishment:*

André Boucher, Associate Deputy Chief, IT Security.

**Thursday, March 22, 2018**

*Morrison & Foerster LLP:*

John P. Carlin, Chair, Global Risk and Crisis Management (by video conference).

TÉMOINS

**Le mercredi 21 mars 2018**

*Institut de la cybersécurité et de la protection des renseignements personnels, Université de Waterloo :*

Florian Kerschbaum, directeur intérimaire.

*Sécurité publique Canada :*

Colleen Merchant, directrice générale, Direction de la cybersécurité nationale.

*Gendarmerie royale du Canada :*

Surintendant principal Jeff Adam, commissaire adjointpar intérim, Opérations techniques.

*Centre de la sécurité des télécommunications :*

André Boucher, chef adjoint associé, Sécurité des TI.

**Le jeudi 22 mars 2018**

*Morrison & Foerster s.r.l. :*

John P. Carlin, président, Risques mondiaux et gestion de crise (par vidéoconférence).